REPORT OF EXAMINATION | 2019M-115

Middleburgh Central School District

Information Technology

DECEMBER 2019

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

Contents

Report Highlights

Middleburgh Central Schol District

Audit Objective

Determine whether the Board and District officials adequately safeguarded data from potential abuse or loss.

Key Findings

- District officials did not adequately manage user accounts and their user permissions. For example, former employees and an unknown person had active accounts, and administrative permissions were granted to individuals who did not need these rights. In two instances, officials did not know why the users had excessive permissions.
- Officials did not provide IT security awareness training to employees, and the Board did not establish a disaster recovery plan.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Periodically review enabled user accounts to ensure they are still needed and limit administrative permissions to those users who need them to perform their job functions.
- Provide employees with formal IT security awareness training and adopt a disaster recovery plan.

District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Middleburgh Central School District (District) serves nine towns and one village in Schoharie County and two towns in Albany County.

The District is governed by a five-member Board of Education (Board). The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible for the day-to-day management under the direction of the Board.

Quick Facts	
Enrollment	745
Employees	180
Desktops, Laptops and Tablets	361
2018-19 Appropriations	$22,169,182

Audit Period

July 1, 2017 – December 12, 2018. We extended our scope to review IT findings and recommendations from the audit that OSC conducted in 2009.

Information Technology

The District employed a computer support specialist (CSS) and two computer support teaching assistants who provided IT support to District staff and students. Also, the District annually contracted with the Northeastern Regional Information Center (NERIC) as part of their cooperative service agreement to provide information technology (IT) services to the District. These services included maintaining and supporting specific applications and managing the District's firewall and intrusion detection system.[1]

District employees must have a NERIC user account to access data for applications supported and maintained by NERIC. NERIC added, deleted and modified these user accounts based on the District's request and approval. In addition, the CSS added, deleted and modified the District's network and local accounts.

Why Should the District Manage User Accounts and Permissions?

Network and local user accounts enable a network and individual computers to recognize specific users and grant authorized permissions to users. However, network and local user accounts can be used as potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI).[2] A district should have written procedures for granting, changing and revoking user access.

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

Generally, a designated administrator has oversight and control of a system or application with the ability to add new users, 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. Therefore, officials must ensure that network accounts with administrative permissions are assigned only to those who need them to perform their job duties.

---

1 A firewall is a software application or hardware device that filters traffic between a trusted network and an untrusted network, such as the Internet. An intrusion detection system (IDS) is a software application or hardware device installed on a network that detects and reports intrusion attempts. A firewall can block a suspicious connection while an IDS cannot.

2 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.

Whenever administrative permissions are needed for an employee's job, officials must ensure that the employee has two user accounts: the administrative account and a user account with lesser-privileged permissions to be used for nonadministrative tasks, such as accessing email and browsing the Internet. This can help protect the network from compromise if the employee encounters malware through Internet-based applications and/or tasks.

Officials Did Not Adequately Manage User Accounts and Permissions

Officials did not properly manage the District's network and local user accounts to safeguard data from potential abuse and loss. We reviewed all 323 nonstudent network accounts[3] and 10 local user accounts on eight computers assigned to eight District employees[4] to determine whether the accounts were active, assigned to current District employees and had proper user permissions and found the following:

Questionable Accounts – We reviewed 255 nonstudent network accounts[5] and found that 59 (23 percent) did not match the 2017-18 employee master list. We reviewed nine of these accounts[6] and found the following:

- Five were former employees whose accounts should have been disabled. The CSS told us he received verbal or written instructions from District administrators to add or disable user accounts and that user accounts were disabled immediately upon receipt of notification from administration. However, he was not instructed to disable these accounts.
- Three were assigned to Capital Region Board of Cooperative Educational Services (BOCES) employees.[7] One was never used, one had not been used in four years and one had not been used within the past year. District officials told us that these accounts were needed accounts. However, based on the timespan since the accounts were used, officials should review the purpose of the accounts and determine whether they should disable them until they become necessary.

3 These accounts included District employee network accounts, nonemployee network accounts, such as those for NERIC employees, and generic accounts. 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. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account.

4 Refer to Appendix B for further information on our sampling selection.

5 We excluded generic accounts from this sample population because they were not associated with specific users.

6 See supra, note 4.

7 The District contracted with the BOCES through its annual cooperative service agreement for a data coach, a lead evaluator and for information technology support, which required these three employees to have District network accounts.

- One was not a District or NERIC employee and was unknown to officials.

Administrative Permissions – The District had 29 network accounts with administrative permissions during our audit period. We reviewed 16[8] to determine whether the users assigned to the accounts needed administrative permissions and found that nine did not need it based on their job duties. For example, the high school principal's daily duties did not include network administration. Therefore, he should not have had the ability to add or delete user accounts from the District's network.

The CSS stated that one user did not need administrative permissions, and he was unsure why two had administrative permissions. He also told us that the remaining 13 users needed administrative permissions to access files, download needed software and "to be more efficient." In addition, none of the 16 users with administrative permissions had a lesser privileged user account for day-to-day activities.

If the 13 users needed to access files and download software, they would not have needed network administrative permissions to do so. The CSS could have given these individuals full access to the files and the ability to download software without granting them full access to the entire network.

District officials told us that user accounts and their user permissions were initially set up by NERIC, and that users were assigned to a group based on prior administrative approval. For example, according to the CSS, District administrators and select employees were assigned to the District's administrator group, which allowed them to access shared files.

User accounts of former employees that have not been disabled could potentially be used by those individuals or others for malicious purposes. Because the District did not have formal procedures for regularly reviewing enabled network accounts, disabling unneeded accounts and periodically reviewing user permissions, its unused accounts and user permissions were not being adequately managed. In addition, because the District's network had unneeded active accounts, it had a greater risk that these accounts could have been used as entry points for attackers to gain access to District data and compromise IT resources.

Why Should Officials Provide IT Security Awareness Training to Employees?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and

8 See supra, note 4.

data and communicates related policies and procedures to all employees and students. The training should center on emerging trends such as information theft, social engineering attacks[9] 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.

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 password; 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.

In addition, the Board and officials should establish a policy and written procedures that require employees to be trained in IT security awareness issues and in proper usage of the IT infrastructure, software and data. While IT policies will not guarantee the safety of the District's systems, without formal policies and procedures that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Officials Did Not Provide IT Security Awareness Training to Employees

Officials did not provide employees with IT security awareness training to help ensure they understood IT security measures designed to safeguard data from potential abuse or loss. While the District's acceptable use policy included some basic guidelines, the Board and officials did not implement administrative procedures requiring employees to be trained in proper usage of the IT infrastructure, software and data.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District 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, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

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

Why Should the Board Adopt a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, District officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus, vandalism, or inadvertent employee action) that could compromise the network and the availability or integrity of the financial systems and any PPSI contained therein.

Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions 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. Backup data should be stored at a secure offsite location, encrypted and routinely tested to ensure its integrity.

The Board Did Not Adopt a Disaster Recovery Plan

The Board did not adopt a comprehensive written plan to describe how officials would respond to potential disasters. Although OSC communicated the importance of an adequate plan to the Board in a prior OSC audit[10] and the former Board outlined procedures to correct this issue, the former Board did not adopt a plan. The current administration was not aware that a plan was never created.

In addition, although backups were performed on a regular basis, the backups of the District's nonfinancial data were not stored offsite. Because the District's buildings are located in a flood plain, the District has a greater-than-average risk that a natural disaster could occur at the District.

Without a plan, officials cannot guarantee that in the event of a disaster they would be able to restore critical IT systems, applications or data in a timely manner. As a result, the District has an increased risk that it could lose important data and suffer serious interruption in operations.

10 *Middleburgh Central School District – Internal Controls Over Selected Financial Operations* (2009M-74, released November 2009)

What Do We Recommend?

The Board should:

1. Develop policies to ensure that unneeded user accounts are disabled in a timely manner and that all users have appropriate network and local user permissions.
2. Adopt a policy requiring employees to receive IT security awareness training, including proper usage of the IT infrastructure, software and data.
3. Adopt a comprehensive, written disaster recovery plan that provides specific guidelines for the protection of data against loss or destruction.

District officials should:

4. Develop formal procedures for reviewing enabled accounts and user permissions and disabling unneeded accounts, including notifying the CSS of individual employment status changes.
5. Regularly review user permissions granted to individuals to determine whether they are appropriate and needed and adjust and/or revoke excessive permissions that are deemed unnecessary.
6. Provide separate user accounts with lesser-privileged permissions to administrators to use for nonadministrative tasks.
7. Ensure employees receive formal IT cybersecurity awareness training on a periodic basis that reflects current risks identified by the IT cybersecurity community.
8. Ensure that the backups of the District's nonfinancial data are stored offsite.

Appendix A: Response From District Officials

MIDDLEBURGH CENTRAL SCHOOL DISTRICT
Office of the Superintendent
291 Main Street – P.O. Box 606
Middleburgh, New York 12122
(518) 827-3625

December 6, 2019

Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear Ms. Singer:

The Middleburgh Central School District is in receipt of the Draft Audit Report based on the critical review of our information technology (IT) security controls, for the audit period of July 1, 2017-December 12, 2018. Please consider this letter as the district's response to the audit.

Upon review of the IT draft audit, the district is in agreement with the report and findings. We have begun to address all of the recommendations in the form of new policies, procedures and protocols to improve our IT infrastructure and management.

On behalf of the Board of Education, we would like to thank the Office of the State Comptroller for their professional service and expertise in conducting this time-intensive and complex audit. We feel that the process was thorough, fair and comprehensive.

Sincerely,

Brian P. Dunn
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 Board's policies, procedures and meeting minutes and interviewed officials to gain an understanding of the District's IT environment and determine whether the policies and procedures in place were adequate.
- We analyzed the District's network accounts and related settings using a computerized audit script. We excluded student network accounts from our analysis because these accounts had greater user restrictions and, as a result, were considered lower risk. We compared the 323 nonstudent network accounts to the active employee list to identify accounts for former employees and/or unauthorized users.
- We used our professional judgment to select a sample of eight employees assigned to eight computers and reviewed their user permissions. We chose these individuals because they had administrative permissions and could potentially access PPSI. The eight computers had 10 local accounts.
- Of the 29 network accounts that had administrative permissions (15 District employee accounts, 12 generic accounts, one NERIC employee account and one vendor account), we used our professional judgment to select the accounts assigned to 16 users for further review. These 16 users included five District employees (30 percent), nine generic accounts (75 percent), one NERIC employee and one vendor. We chose to review the five District employee and nine generic accounts based on the potential access these accounts had to PPSI and the District's financial system data. We reviewed each users' job responsibilities and discussed their administrative permissions with District officials to determine whether their user permissions were needed.
- We compared the full names of all nonstudent network accounts to the full names of employees who were actively employed by the District during the 2017-18 school year and found 59 unmatched names. We used our professional judgment to select every sixth name from the list of 59 unmatched names for further review. This gave us a total sample of nine names. We discussed the status of these employees with District officials.
- We reviewed available documentation to determine whether officials were monitoring and/or enforcing the Board's IT policies and procedures and whether IT security awareness training was provided to employees who used the District's IT resources.

- We followed up on the findings and recommendations from a prior OSC audit of the IT system to determine whether officials corrected the weaknesses identified.[11]

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 officials.

We conducted this performance audit in accordance with GAGAS (generally accepted government auditing standards). 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.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the District clerk's office.

11 See supra, note 10.

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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

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