DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION 2020M-112

Honeoye Falls Lima Central School District

Access Controls

FEBRUARY 2021

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

Contents

Report Highlights

Honeoye Falls Lima Central School District

Audit Objective

Determine whether Honeoye Falls Lima Central School District (District) officials ensured user access controls were appropriate and designed effectively.

Key Findings

District officials did not ensure user access controls were appropriate and secure. Officials did not:

- Adopt key information technology (IT) security policies, resulting in increased risk that data, hardware and software may be lost or damaged by inappropriate use or access.
- Regularly review network user accounts and permissions to determine whether they were appropriate or needed to be disabled.

In addition, sensitive IT control weaknesses were communicated confidentially to officials.

Due to the COVID-19 pandemic, with the District's increased reliance on a remote learning environment and administrative operations, protecting IT assets is critical.

Key Recommendations

- Adopt and enforce comprehensive IT security policies.
- Regularly review network user accounts and disable those that are unnecessary.

District officials generally agreed with our recommendations and indicated they would implement corrective action.

Background

The District serves residents in the Towns of Avon, Lima and Livonia in Livingston County, Henrietta, Mendon and Rush in Monroe County and Richmond, Victor and West Bloomfield in Ontario County.

The nine-member Board of Education (Board) is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the District's administration.

District officials and staff rely on the District's IT assets for Internet access, email and maintaining confidential and sensitive financial, student and personnel records. The Director of Technology Services (Director) is the network administrator and is assisted by several IT staff and BOCES with the day-to-day IT operations.

Network User Accounts Quick Facts	
Enabled	2,921
Student	2,252
Nonstudent	669

Audit Period

July 1, 2018 – July 31, 2020

Access Controls

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, such as those related to user accounts and permissions, security awareness, data breach and classification and business continuity. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the district. Finally, officials should periodically review these policies, update them as needed and designate personnel who are responsible for monitoring policy compliance.

District officials should have an acceptable computer use policy (AUP) that defines procedures for acceptable computer, Internet and email use and specific consequences for violations. District officials can reduce the risks to personal, private and sensitive information (PPSI)[1] and IT assets by 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 Board adopted an AUP and online banking policy, it did not adopt other IT security policies and procedures to address key IT security issues, such as those related to user accounts and permissions, security awareness, data breach and classification and business continuity.

The AUP allows users to connect personally-owned equipment to the District's network and allows for the personal use of social media during District time on District-owned equipment on a limited basis. However, the policy does not define what the District considers acceptable personal use, does not define limited basis and does not include penalties for violation of this policy. Officials stated they are in the process of reviewing IT standards and are prioritizing the District's need to adopt additional IT policies.

We reviewed the Internet browsing histories on 18 computers[2] and found questionable Internet use on 12 computers, two of which had excessive personal use. Users of these computers accessed non-school-related websites used for

1 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.

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

online shopping, accessing a players club gambling account, personal online banking, personal email, music and video streaming, various news and websites, and searches for jobs and real estate. Users may have been unaware that accessing these non-school-related websites could compromise PPSI and IT assets.

Nine of the 18 computers contained evidence of current or previous malicious software infections or potentially unwanted program (e.g., spyware, adware) installations. Malicious software can result in issues that range from a nuisance (e.g., pop-up messages) to theft of personal information (e.g., social security numbers) or a completely inoperable computer (e.g., locked, encrypted or corrupted system). Potentially unwanted programs can sometimes lead to similar issues, and can unnecessarily consume system resources and decrease productivity when used by employees.

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

Why Should the District 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.[3] The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the IT system and data, including its financial application and any PPSI contained therein.

Typically, a plan involves analyzing business processes, 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 address changes in security requirements.

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

The District Did Not Have a Disaster Recovery Plan

The Board did not develop a comprehensive formal disaster recovery plan to describe how officials would respond to potential disasters affecting IT. Consequently, in the event of a disaster, phishing[4] or a ransomware attack, staff had no guidance to follow to restore or resume essential operations in a timely manner. Without a formal plan, there is an increased risk that the District 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 District officials told us that the financial data is backed up regularly, and backups are stored offsite, the backups have not 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.

Why Should Officials Manage User Accounts and Permissions?

District officials are responsible for restricting network and local 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.

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users. Network user accounts are potential entry points for attackers because, if compromised, they could be used to access and view data stored on the network. When multiple users are allowed to share network user accounts, the district 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 user accounts are no longer needed, they should be disabled in a timely manner. The district should have written procedures for granting, changing and removing user access and permissions to the overall networked computer system.

When user accounts are no longer needed, they should be disabled in a timely manner.

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

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

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 Network User Accounts and Permissions

When an employee separates from the District, the human resources department emails IT staff to remove the user's network access. In addition, IT staff stated they perform a semi-annual review of network user accounts and make any necessary changes at the time of their review.

Although procedures were in place, District officials did not adequately manage network user accounts and permissions for the District's network. As a result, the District had unneeded, unused and shared accounts that had not been disabled and/or monitored.

Unneeded/Unused Network User Accounts – During our review of 669 nonstudent network user accounts, we found that 188 user accounts (28 percent) had not been used in at least six months. Also, 62 of these accounts had never been used. Officials stated these accounts are for employees that had not been working since the District closed due to the pandemic. However, at the time of our testing, the District had been closed for approximately two months, leaving four months of unexplained inactivity by these users.

Although District officials have a process for removing employees' access upon separation or when no longer needed, we found removal was not always timely. For example, we identified 281 potentially unneeded user accounts on the April 22, 2020 enabled user account list, which District officials stated 156 were unneeded and would be removed by May 18, 2020. However, the May 29, 2020 enabled user account list still included 31 of the 156 users. Officials told us they have subsequently deleted the 31 user accounts. Another example included an employee that separated from District employment on April 14, 2020, but still had an enabled user account on the April 22, 2020 enabled user account list. This user was removed from the May 29, 2020 enabled user account list. When unnecessary user accounts are not removed in a timely manner, the risk of unauthorized access to the District's network is increased.

Unneeded Generic[5] and/or Shared Accounts – During our review of 669 nonstudent network user accounts, we found that 119 accounts were generic and/or shared accounts[6] and 78 of these accounts were not used in the last six months. Officials stated these accounts are necessary to access applications on the network and were for employees that had not been working since the District closed due to the pandemic. However, at the time of our testing the District had been closed for approximately two months, leaving four months of unexplained inactivity by these employees.

Unneeded network user accounts can be potential entry points for attackers because they are not monitored or used and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. Also, when the District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access. In addition, if users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Administrative Permissions – During our review of 19 local user accounts,[7] we found that 18 user accounts had administrative permissions. In addition, 15 of 18 computers tested allowed network user accounts that are a part of an office staff user group (containing seven users) and/or a teacher user group (containing 54 users) to have local administrative rights. Also, six of 18 computers allow network accounts in a staff user group (containing 543 users) to have local administrative access as well. This means that users that are part of these groups have administrative rights on more than just their computers. A few members of these groups include sport coaches, food service workers, lunch monitors and maintenance/cleaners. According to the Director, the District allows all local users to have administrative permissions to their computers, but did not provide a further explanation.

When users have unneeded administrative permissions to networks and computers, 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 use those elevated privileges to cause greater damage than with a lesser-privileged account.

When users have unneeded administrative permissions to networks and computers, they could make unauthorized changes that might not be detected.

5 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.

6 The shared accounts were being shared among various users.

7 We reviewed 18 computers and one computer had two local user accounts, resulting in 19 local user accounts.

Why Should the District Have a Service Level Agreement (SLA) With Its IT Service Provider?

District officials must ensure that they have qualified IT personnel to manage the district's IT environment. This can be accomplished by using district employees, an IT service provider or both. To protect district assets and avoid potential misunderstandings, officials should have a written SLA with the district's IT service provider that clearly identifies the district's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI.

An SLA is different from a traditional written contract in that it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The SLA should be reviewed by knowledgeable IT staff, legal counsel or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

District Officials Did Not Have an SLA With BOCES

District officials provided unrestricted remote access to BOCES staff to provide various IT-related services such as network technical support, IT support and management, Internet filtering, backups and firewall/intrusion detection. However, officials had no policies or procedures in place to monitor and review the work performed by BOCES staff or ensure the District's IT assets and data were safeguarded.

In addition, District officials stated there was no formal agreement or SLA with BOCES to identify the vendors' responsibilities and specific services to be provided because it was unaware of the benefits of having such agreements. Instead, District officials chose IT products and services by selecting certain items from a list of available services provided by the vendor. However, the list did not provide detailed explanations of the services.

Also, they could not have compared whether they were receiving the best value for similar goods and services offered by other IT vendors. Without a written SLA, the District and BOCES did not have stated responsibilities and procedures for how to resolve any failures in IT controls, such as a service disruption or data

breach. This can contribute to confusion over who has responsibility for the various aspects of the District's IT environment, which could put the District's computer resources and data at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies to address user accounts and permissions, security awareness, data breach and classification and business continuity.
2. Consider amending the AUP to allow only District-owned assets to connect to the District's network, clearly define what an acceptable level of personal use is, and identify penalties for violation of this policy.
3. Develop an SLA with BOCES to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties.

District officials should:

4. Develop and adopt a comprehensive disaster recovery plan, including data backup procedures and off-site storage.
5. Assess network and local user accounts and permissions on a regular basis and remove or disable unnecessary accounts and excessive user permissions for those users who do not need that level of access to perform their current job duties.

Appendix A: Response From District Officials

HONEOYE FALLS-LIMA
Central School District
Dr. Bruce Capron, *Assistant Superintendent for Business & Operations*
Office: (585) 624-7020
Fax: (585) 624-7003
E-mail: bruce.capron@hflcsd.org

"Education is the Foundation for Success"

December 4, 2020

The Honeoye Falls – Lima School District appreciates the auditing work the Office of the State Comptroller's team did to evaluate our computer and network systems. The district agree that IT security and cybersecurity are critical areas of our operations. Our school district is seeking to follow best practices regarding identifying risks, setting policies and regulations, and developing appropriate mitigations aligned with the NIST security framework. Our goal is to balance having students and staff find ways to creatively use technology to optimize teaching and learning while simultaneously securing our IT infrastructure from threats.

The District appreciates and generally agrees with all of the recommendations that include:

1. Adopting comprehensive IT security policies and regulations;
2. Amending our network AUP and permissions regarding non-district devices;
3. Creating a service level agreement with our BOCES that clearly defines roles and responsibilities;
4. Developing a comprehensive disaster recovery plan; and
5. Developing procedures and regulations to better monitor user accounts and permissions.

A more detailed response to each audit recommendation along with our proposed corrective actions is provided in following pages.

Sincerely,

Bruce Capron

Unit Name: Honeoye Falls-Lima CSD
Audit Report Title: Access Controls
Audit Report Number: 2020M-112

Public Audit Recommendation #1
Adopt comprehensive IT security policies to address user accounts and permissions, security awareness, data breach and classification and business continuity.

Implementation Plan of Action: *Tentative list of policies/regulations to write*

The following programs have been identified as the most critical to operations and contain the most sensitive data. The district is prioritizing developing IT security policies and regulations for these programs.

- Technology & HR: new/moving/exiting staff process - in progress
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Implementation Date:
Technology Director will work with appropriate staff to complete 3 policies per month to be completed by July 1, 2021

Person Responsible for Implementation

Technology Director

Signed:

Title: Director of Technology

Date: December 4, 2020

Unit Name: Honeoye Falls-Lima CSD
Audit Report Title: Access Controls
Audit Report Number: 2020M-112

Public Audit Recommendation #2

Consider amending the AUP to allow only District-owned assets to connect to the District's network, clearly define what an acceptable level of personal use is and identify penalties for violation of this policy.

Implementation Plan of Action

Technology Team is recommending the following action:

The AUP will be modified to prohibit any personal device (non-HF-L owned device) to connect to HF-L wireless or a wired connection.

Students and staff who bring their personal devices to school will have access to the guest wireless network only.

Implementation Date

January 1, 2021
Send notification to students and staff prior of the change

Person Responsible for Implementation

Network Administrator
Technology Director

Signed:

Title: Director of Technology

Date: December 4, 2020

Unit Name: Honeoye Falls-Lima CSD
Audit Report Title: Access Controls
Audit Report Number: 2020M-112

Public Audit Recommendation #3

Develop a Service Level Agreement (SLA) with BOCES to address the District's specific needs and expectations for IT services and the roles and responsibilities of all part

Implementation Plan of Action

The Technology Director will work with BOCES and other component schools and RICS to develop a plan. (As discussed with OSC auditors, since this is a state-wide issue for most BOCES and component schools, the district would appreciate receiving any model agreements or templates to support this work.)

Implementation Date

This is a regional and statewide issue. with a target date of Aug 31, 2021.

Person Responsible for Implementation

Technology Director
BOCES

Signed:

Title: Director of Technology

Date: December 4, 2020

Unit Name: Honeoye Falls-Lima CSD
Audit Report Title: Access Controls
Audit Report Number: 2020M-112

Public Audit Recommendation #4

Develop and adopt a comprehensive disaster recovery plan, including data backup procedures and off-site storage.

Implementation Plan of Action

The Disaster Recovery plan is part of the NIST standards work and is currently in progress

Implementation Date

Target date for completion – August 2021

Person Responsible for Implementation

Technology Director
Entire Technology Department
BOCES

Signed:

Title: Director of Technology

Date: December 4, 2020

Unit Name: Honeoye Falls-Lima CSD
Audit Report Title: Access Controls
Audit Report Number: 2020M-112

Public Audit Recommendation #5

Assess network and local user accounts and permissions on a regular basis and remove or disable unnecessary accounts and excessive user permissions for those users who do not need that level of access to perform their current job duties.

Implementation Plan of Action

Technology Director has implemented a monthly schedule at which time the Network Admin reviews the following logs and meets with the Technology Director to review results and adjusts as needed.

The following logs are currently being reviewed:
Active Directory logs for accounts inactive for 30 days or more, as well as access level review.
Door Access/Badging system logs to verify accuracy in access levels and current staff.

This plan will integrate with HR policies and student policies related to exiting the district, leaves, and role changes and incorporate responsibilities of IT and direct supervisors.

Implementation Date

November 2020 and will continue

Person Responsible for Implementation

Network Admin
Tech Director

Signed:

Title: Director of Technology

Date: December 4, 2020

Appendix B: Audit Methodology and Standards

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

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of IT operations, specifically those related to the granting, modification and revocation of network and local user accounts and permissions.
- We used various local, network and application user lists to assign a level of risk to each user. Each user's risk level was based on their access to and permissions within the various applications and their role and title at the District, including their ability to access PPSI. Administrators at the District and administrators of the various software packages were deemed to have higher risk than non-administrators. We used our professional judgment to categorize users into five levels of risk and selected 20 users for testing. Our sample of 20 users was comprised of the following: nine users (100 percent in these categories) from the two highest risk categories, seven users (20 percent in this category) from the middle risk category and four users (1 percent in these categories) from the two lowest risk categories.
- District officials informed us that two of the 20 users selected did not have a designated computer assigned to them. As a result, our computerized audit scripts were only executed on 18 computers.
- We provided the Director with computerized audit scripts to run on the 18 computers and she provided us copies of the reports and files generated by the scripts. We analyzed these reports and files to obtain information about the District's nonstudent network users to determine whether user account and security settings were necessary and appropriate. We reviewed user accounts and compared them to a list of current employees to identify potentially inactive and unnecessary accounts. We also analyzed user accounts and security settings applied to those accounts on the District's servers. In addition, we reviewed the Internet use on the 18 computers we selected for testing to evaluate whether their Internet use was in compliance with the District's AUP and if unnecessary exposure occurred.
- We followed up with District officials on possibly unneeded accounts and automated settings that indicated ineffective IT controls.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan

and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-1(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 next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

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

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/cyber-security-guide.pdf

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

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

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

Contact

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

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

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

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

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