REPORT OF EXAMINATION | 2021M-134

Pelham Union Free School District

Information Technology

APRIL 2022

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

Contents

Report Highlights

Pelham Union Free School District

Audit Objective

Determine whether Pelham Union Free School District (District) officials established adequate controls over user accounts to help prevent unauthorized use, access and loss, and adopted an adequate IT contingency plan.

Key Findings

District officials did not establish adequate controls over user accounts to help prevent against unauthorized use, access, and loss, and did not adopt an adequate IT contingency plan. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, officials did not:

- Periodically review unneeded user accounts and permissions to determine whether they were appropriate or needed to be disabled.
  - 33 individuals who left employment and 221 students who were no longer enrolled had active network user accounts.
  - Three generic accounts were not needed for District operations.
  - Four user accounts had unnecessary permissions.
- Ensure the District's IT contingency plan was comprehensive, distributed and tested to minimize the risk of data loss or prevent a serious interruption of services.

Key Recommendations

- Develop written procedures for managing network and financial application user account access and develop and adopt a comprehensive IT contingency plan.

District officials agreed with our recommendations and indicated they plan to initiate corrective action.

Background

The District serves the Town of Pelham in Westchester County.

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

The Superintendent is the chief executive officer and responsible, along with other administrative staff, for day-to-day operations.

The District's Information Technology Director (IT Director) is responsible for overseeing the acquisition and use of District computer resources. The District contracted with the Lower Hudson Regional Information Center (LHRIC) for IT infrastructure and the operation of a service desk to address IT issues that arise.

Quick Facts	
Students	2,807
Employees	528
Network Accounts	
Student	2,999
Employee	504
Generic	57
Total	3,560

Audit Period

July 1, 2019 – November 30, 2020

Information Technology

The District's IT system and data are valuable resources. The District relies on its IT assets for a variety of tasks, including Internet access, email, and for maintaining financial, personnel and student records, which contain personal, private and sensitive information (PPSI).[1] If the IT system is compromised, the results can be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls do not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use and loss.

... [D]istrict officials should actively manage network and software application user accounts to ensure they are appropriate and still needed.

How Should Officials Properly Manage User Accounts?

User accounts provide access to a district's network and software applications and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers to inappropriately access and view PPSI on the network.

A district should have written procedures for granting, changing, and disabling access to the network and specific software applications. These procedures should establish who has the authority to grant or change access and allow users to access only what is necessary to complete their job duties or other assigned responsibilities.

To minimize the risk of unauthorized access, district officials should actively manage network and software application user accounts to ensure they are appropriate and still needed. Officials must disable unnecessary or unneeded accounts as soon as there is no longer a need for them.

Officials Did Not Adequately Manage User Accounts

District officials did not develop comprehensive written procedures for managing network access and financial application permissions, such as procedures to grant, change, and disable access to the network and specific software applications, periodically review user accounts and disable network accounts when access was no longer needed and ensure permissions to the financial application software were necessary for employees to complete their job duties.

The District Treasurer (Treasurer) said the District is small, readily aware of staffing changes and works with the IT department to perform timely removal of permissions to the financial application. However, the IT Director, who was responsible to ensure user accounts were appropriately managed, told us he was not always informed when network users left District employment.

1 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.

Unneeded Employee User Accounts – We reviewed all 504 employee network users accounts for inactive user accounts (accounts that have not logged into the network for at least six months before December 22, 2020). We identified 39 employee network user accounts that were not needed. The 39 unneeded employee user accounts included:

- 33 employees who left District. These former employee accounts were inactive from six months to more than a year.
- Four employees who occasionally worked for the District but were not currently employed by the District.
- A former Board member who no longer served the District and never logged onto the network. The account was created in May 2019 and was never used as of December 22, 2020.
- A deceased employee whose account was not removed.

The IT Director told us he was not always informed when employees leave the District and he forgot to disable the access of the employee who passed away. The IT Director said that he can use extra staff to assist with oversight of controls over user accounts.

Unneeded Student User Accounts – We reviewed all 2,999 student network user accounts and identified 221 accounts that were unneeded because they were assigned to students no longer enrolled at the District. We also found 32 students enrolled that did not have a network user account and three accounts were duplicates on the network. The 221 unneeded student user accounts include:

- 156 accounts that students never logged into.
- 65 student accounts were not recently logged into. Following is a breakdown of the last time these accounts were logged into:
  - Nine in 2018
  - 54 in 2019
  - One in January 2020
  - One in March 2020

The IT Director said in January 2020, they started an automated removal process when students leave the District that communicates to the network. He was unaware that there were students on the network that were not enrolled.

Unneeded Generic Accounts – We reviewed all 57 generic accounts and discussed with the IT director to assess whether they were necessary for District operations and we found that three were unneeded. These accounts included one organization fund account and two accounts used for testing by IT department personnel.

Financial Application User Permissions – We reviewed all 39 accounts with permissions to the financial application. We found four users with unnecessary permissions that were inconsistent with their job responsibilities. Two of these permissions provided users with unnecessary access to PPSI. The following users had such permissions:

- A secretary and an internal auditor had access to a retirement module that did not relate to their job duties. They were able to create, delete and update New York State and Local Retirement System and New York State Teachers' Retirement System reports. The Treasurer told us the internal auditor should only have read access capability and the secretary should not have any access to the retirement module.
- A clerk had access to delete purchase requisitions and did not have that job duty.
- An administrative assistant and the secretary had access to dates of birth, personnel files, and employee health benefits, but did not need to have these permissions for their job duties.

The Treasurer told us the employees should not have these permissions and they were not aware of this access. As a result, there is a risk of exposure of PPSI and there is an increased risk that intentional or unintentional changes to the financial application could occur without detection.

Without formal procedures for regularly reviewing enabled user accounts, the District had a greater risk that the unneeded accounts could be compromised or used for malicious purposes.

Unneeded network user accounts and financial application permissions must be disabled promptly to decrease the risk of unauthorized access and potential entry points for attackers

Why Should a District Adopt an IT Contingency Plan?

An IT contingency plan is a district's recovery strategy, composed of the procedures and technical measures that enable the recovery of IT operations after an unexpected incident. An unexpected incident could include a software failure caused by a virus or malicious software or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable therefore, it is crucial to plan for such an event.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of a district's computer operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to enable the recovery of a computer system and/

The goal of an IT contingency plan is to enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

or electronic data as quickly and effectively as possible following an unplanned disruption.

Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining an organization's critical business processes in the event of a disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Policies and procedures are also critical components and ensure that information is routinely backed up and available in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by the organization, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested.

The District's Plan Was Not Adequate, Distributed or Recently Tested

Although officials had a disaster recovery plan (plan) in place, it was inadequate and not comprehensive. The IT Director did not know a disaster recovery plan existed until we inquired and asked for a copy. Consequently, in the event of a disruption, a disaster, phishing[2] or a ransomware attack, employees have inadequate guidance to follow to restore or resume essential operations in a timely manner. Without a comprehensive 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.

The plan appeared to be a standard template that was not completed by District officials and did not list the District's information, the emergency planning team, staff in charge of specific roles, and the District checklist. The annual review

2 Phishing is deceptive email messages that attempt to gather personal information or infect computer systems with malicious software.

period was not updated, and the plan's key contact list was last updated in 2013. The names listed in the plan included former officials, such as the former Superintendent, Assistant Superintendent for Business, and the IT Director.

In addition, the plan was not periodically tested (with exception of 911 phone system) to ensure key officials and District contractors understood their roles and responsibilities in a disaster situation and to address changes in security requirements. We asked officials currently in those key positions whether the plan was distributed to them and they said it was not and that they did not receive any training on the plan.

Additionally, the plan did not identify current critical business processes and services, there were no details provided on how often the plan should be tested or updated. Further, the plan did not include, and the District did not have, a backup policy or procedures describing how officials would restore critical IT system data.

Although District officials had a backup procedure for the financial software application, the procedure was ineffective because it was not distributed to key officials. The IT Director and LHRIC representative told us backups were completed weekly and periodic restoration was performed once or twice every 15 days. However, the officials did not provide documentation showing the backups were periodically restored successfully to ensure the process is functioning as intended and that data would be available in an emergency.

Without an updated comprehensive contingency plan in place that is distributed to all responsible parties and periodically tested for effectiveness, District officials have less assurance that employees will react quickly and effectively to maintain business continuity in the event of a disruption or other event impacting operations.

In addition, without a backup policy and periodic testing of backups the officials cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurs. IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations.

IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost. ...

What Do We Recommend?

District officials should:

1. Develop written procedures for managing network and financial application access, such as procedures to grant, change, and disable access to the network and specific software applications and periodically review user access and disable user accounts when access is no longer needed.

2. Periodically review financial application access and limit access to ensure that access is based on job function.

3. Develop, adopt, distribute and periodically update and test a comprehensive IT contingency plan that includes detailed guidance for continuing operations, key personnel and procedures for recovery of IT operations.

Appendix A: Response From District Officials

PELHAM PUBLIC SCHOOLS

Dr. Cheryl H. Champ
Superintendent of Schools

629 Fifth Avenue
Pelham, New York 10803

914 738-3434 ♦ Fax 914 738-7223
cchamp@pelhamschools.org

March 28, 2022

Ms. Lisa Reynolds
Chief Examiner of Local Government and School Accountability
State of New York
Office of the State Comptroller
110 State Street
Albany, NY 12236

Dear Ms. Reynolds:

The Pelham Union Free School District is in receipt of your draft Information Technology Report of Examination 2021M-134 covering the audit period July 1, 2019, through November 30, 2020.

We sincerely thank the Office of State Comptroller for this opportunity to examine our information technology (IT) systems, as the District places the highest priority on maintaining and improving the security of our data systems, especially in an environment in which threats and risks to IT systems and data are an everyday reality. Further, we wish to acknowledge our appreciation for the professional and collaborative field staff who conducted the audit work.

The District agrees with the Comptroller's recommendations to develop written procedures for managing network and financial application access, to periodically review financial application access, and to develop, adopt, distribute and periodically update and test a comprehensive IT contingency plan. Since the time of the audit period under review, the District had already implemented some of these suggested improvements. The District is preparing a corrective action plan which will outline the actions taken and to be taken in response to the Comptroller's findings. This plan will be presented to the District's Audit Committee and Board of Education for approval.

We would like to acknowledge the strength of our IT department which, while maintaining day-to-day technology demands, has diligently undertaken many significant projects in the past several years under the direction of our IT Director who joined us in 2018. Most notably, we pivoted to a remote learning environment in the face of the COVID-19 pandemic, built a brand new state-of-the-art elementary school, moved administrative offices requiring technology upgrades, implemented a 1:1 device program in grades 2-12, and made significant safety/security improvements District-wide. This department is high performing and continually reviewing practices and policies to ensure that we are following industry standards and best practices.

Again, we sincerely appreciate the work of the Comptroller's Office on our behalf. We will utilize this valuable feedback to further strengthen our IT environment.

Respectfully submitted,

Cheryl H. Champ, Ed D.
Superintendent of Schools

CHC/pd

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 interviewed District officials to gain an understanding of the District's IT operations and reviewed IT related policies to gain an understanding of the IT environment.
- We reviewed user account permissions for all 39 active users of District's financial application to determine whether they were appropriate and based on job functions.
- We used specialized audit script to examine the District's domain controller.[3] We then analyzed the report to determine whether all users were currently employed by the District. We analyzed all generic accounts by following up with District officials to determine which ones were needed. We further analyzed student accounts based on not having a student ID to identify accounts that were no longer needed. We then reviewed the network user accounts and relevant security settings configured on the District's network.
- We obtained the disaster recovery plan from the District officials and reviewed the plan to determine whether it was comprehensive, recently updated, distributed to staff and periodically tested to ensure critical issues were identified.

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 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.

3 The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain. It is responsible for allowing users to access Microsoft Windows domain resources.

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-a (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/files/local-government/pdf/regional-directory.pdf

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

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

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

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

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

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

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

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

Contact

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

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

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

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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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