PELHAM UNION FREE SCHOOL DISTRICT
Corrective Action Plan Related to
COMMUNICATION OF INTERNAL CONTROLS OVER FINANCIAL REPORTING
June 30, 2019

In the course of planning and performing their audit of the financial statements of the Pelham Union Free School District as of and for the year ended June 30, 2019, PKF O'Connor Davies our external auditor, made the following observations about the internal controls and operations, none of which were considered material weaknesses. The District's action plan in response to each deficiency is noted.

EXTRACLASSROOM ACTIVITIES

***FINDING:* Segregation of Duties**

During the audit testing, it was noted that the Central Treasurer for the Middle School Extra Classroom Fund has the ability to collect cash, issue receipts, prepare bank deposit slips, make bank deposits, write checks, and prepare bank reconciliations.

Recommendation

We recommend that the School District takes care to review its segregation of duties framework and ensure that the duties of each employee are truly segregated.

Action Plan

The District has mitigating controls in effect to offset the segregation of duties concerns noted. For instance, the District Treasurer signs all disbursements made by the Middle School Extra Classroom Fund (Fund) and reviews bank statements for the Fund. The Central Treasurer has been instructed to provide adequate documentation on cash receipt records to evidence that all funds collected were deposited. In addition, the Central Treasurer has been asked to prepare year end statements for those clubs with financial activity and to obtain approval of those statements from club advisors. In Fall 2018, the District's internal audit firm performed detailed testing of the Fund. Recommendations made as a result of this work have been considered and, as practical, implemented.

***FINDING:* Inactive Clubs**

During the course of the 2018-19 year, seven clubs had no activity: DIY-Do It Yourself Club ($150), Military History ($1,072), Peer Leadership ($143), Newspaper Club ($30), Robotics ($86), SCI Olympiad ($1,127) and the Youth to Youth Club ($611).

Recommendation

We recommend that the School District evaluate whether these clubs should remain active clubs, or if their funds should be dissolved into another club.

Action Plan

The High School principal and the Central Treasurer review club activity at year end. Typically, a few clubs are closed annually with any remaining fund balances transferred to the general Student Association. Certain clubs remain operationally active while having no financial activity. In such cases, the club fund balance can carryforward without change to ensuing years.

SCHOOL LUNCH FUND

***FINDING:* Excessive Fund Balance**

The School Lunch Fund is used to account for revenues and expenditures in connection with the School District's food service program. New York State Education Regulations suggests that assigned fund balance in the School Lunch Fund be no more than three months' worth of operating average expenditures. The average three month expenditure for the School District is approximately $282,000 and the District has a total unassigned fund balance of approximately $377,000 at June 30, 2019, which is in excess of $95,000.

Recommendation
We recommend that the School District develop a plan to utilize the excess fund balance of the School Lunch Fund to comply with the New York State Education Regulations.

Action Plan
The District is aware of the operating surplus, and is working toward a number of initiatives to reinvest any excess funds into the District's food service program. The District works with NYSED on developing and obtaining approval for a spending plan when the fund balance exceeds allowable limits.

INFORMATION TECHNOLOGY

FINDING: Risk Assessment
We noted that the Organization has not implemented a formal IT risk assessment process.

Recommendation
We recommend that the Organization conduct a formal IT risk assessment as soon as possible and then annually thereafter. The risk assessment should be used to establish and enhance a student electronic data security program and be inclusive of current cyber threats.

Action Plan
The District conducted a risk assessment during the 2017-18 school year and plans to perform periodic assessments on an ongoing basis. The results were used to inform the current draft disaster recovery plan, which will be further refined based on guidance from NYSED with respect to NYS Education Law Section 2-(d).

FINDING: Password Policy
We reviewed the design and implementation of the password controls of the Organization to ensure that the controls in operation would reasonably protect against unauthorized access to system, network, and application resources. We noted the following:

- Passwords have a minimum character requirement of 7 characters. Current best practice is 8 characters minimum.
- Accounts will not lock after repeated failed password entry attempts (locking an account will prevent additional authorization attempts).

Recommendation
We recommend the following minimum password parameters:

- Passwords have a minimum character requirement of at least 8 characters long.
- Accounts should lock after no more than 5-10 password entry attempts.

Action Plan
The District is evaluating this recommendation in light of its varied user groups (administrators, teaching staff, and K-12 students).

FINDING: Server Patch Management
Patches are software or operating system updates issued by a vendor to address security and/or functionality problems. Patch management is the collection of processes to ensure that necessary patches are acquired, tested, distributed for installation, and the status of installation monitored and reported on. The Organization has a patch management process; however, we observed that the frequency and consistency of the patch management methodology was less than effectively operated for servers during the audit period. As such, we identified a set of authentication systems that were out of date and/or not consistently updated with vendor security patches.

Recommendation

We recommend that the Organization ensure all security related patches are installed on a monthly basis. Any deviations of update installation should only be performed after the risks of delaying the installation of the updates are assessed and identified as acceptable to the Organization.

Action Plan

The District's server patch management is overseen by the Lower Hudson Regional Information Center (LHRIC). Patches are applied on a monthly schedule, with critical patches applied immediately when necessary. District personnel will ensure that this work is performed consistently and as scheduled.

***FINDING:* Cybersecurity Awareness Training**

Employees across all business segments poise a significant risk to the security of the network and sensitive data. While technical controls can and should be implemented to limit and control the cyber risk, ultimately employee awareness training is proven to be the most effective mitigation. Further, many types of cyber-attacks are specifically designed to commit financial fraud by leveraging employee cyber education weaknesses. Currently, the Organization does not have a formal cybersecurity awareness-training program.

Recommendation

We recommend the Organization develop and implement a formal employee cybersecurity awareness-training program.

Action Plan

The District mandated student data privacy training for all employees effective with the 2019-20 school year. In addition, the technology department has planned staff training as part of faculty meetings throughout the year.

***FINDING:* IT Standard Operating Policies and Procedures**

We interviewed the IT Director to assess departmental procedures and requested documentation in support of those procedures. We noted that the Organization does not have a set of standard operating policies and procedures. The lack of formally approved, implemented and distributed detailed policies and/or procedures increases the risk that management expectations and control considerations are not followed consistently. As a result, there is an increased risk that personnel could make errors while carrying out information technology and systems functions. Due to the lack of documentation, there is also an increased risk of operation disruption in the absence of key IT personnel.

Recommendation

We recommend that the Organization create a formal set of policies and procedures and distribute them to all necessary employees.

Action Plan

The District currently has an active Policy Committee which continues to review its policies, and to amend them, when necessary. Further, in many cases, underlying regulations exist. The District will review its current IT operating policies in light of this recommendation.

***FINDING:* Environmental Security**

We reviewed the basic environmental controls of the Organization's server and communication room. Environmental controls, such as electrical current conditioning and temperature, are critical in ensuring the uninterrupted operations of the Organization's systems and network. In our review of the communication room, we observed the absence of uninterruptable power supplies ("UPS") on one of the racks housing network communication devices. UPS devices provide both power conditioning and battery backup in case of power fluctuations or loss. With the potential for the organization to experience brownouts throughout the year, the lack of a UPS increases the likelihood of network and communication equipment shutting down abruptly. Additionally, power fluctuations that are not filtered to protect against occurrences such as power spikes, could result in the destruction of the devices resulting in operational downtime. Additionally, in our review of the communication room, we observed the absence of a fire/smoke detector, and a fire suppression system. Should a fire initiate in the room, the server room and data would be at risk; however, more significantly, the entire building would be at risk.

Recommendation
We recommend that the Organization consider connecting all systems and network devices in the communication room to a UPS device, and on a broader scale, we recommend that automatic processes be put into place to insure graceful shutdown of all systems should extended periods of power outage occur. We also recommend that the Organization consider implementing both fire/smoke detectors, and a fire suppressant system in the communication room.

Action Plan
The Distict will closely reassess the existing infrastructure in the communications and server rooms to ensure that all systems and devices are appropriately protected against environmental security threats.

FINDING: **Business Continuity/Disaster Recovery**
We noted that although the Organization has a draft Disaster Recovery plan in place, the plan has not been reviewed, keep current, nor formalized. Without a current formal plan and policy that will dictate and clarify the roles, responsibilities, and steps necessary for the Organization to perform in the event of a disaster, the Organization is at risk for failure to successfully and quickly recover.

Recommendation
We recommend the following to mitigate the risk of failure to recover:

- Management should conduct a formal assessment to determine how long they can be without their functioning servers. In addition, management should assess how much data can be safely lost before there is significant financial, and operational impact. Management should review their operationally critical systems, and based on their acceptable level of risk, prioritize the systems in the order of recovery time (systems that need immediate recovery verses systems that can wait).
- Management should formally document all roles, responsibilities, and procedures necessary to accomplish the transition to the recovery site. Standard disaster recovery documents and plans consist of the following phases: Initiation, Activation, Recovery, and Reconstitution.
- Management should periodically test this plan for functionality as well as practicality.

Action Plan
The District is in the process of updating the disaster recovery plan, with a goal completion date of December 2019. In terms of Business Office operations, the District performs a periodic disaster recovery exercise at LHRIC to ensure that the District's business operations (vendor payment, payroll, online banking, etc.) may continue uninterrupted in the event that normal onsight business operations are interrupted.