CORRECTIVE ACTION PLAN

Glen Cove City School District, New York

Control Deficiencies

- **Extraclassroom Activity Funds**

  Extraclassroom activity funds, which are authorized by the New York State Department of Education, are an integral part of the educational program of the School District. As part of our audit, we have reviewed, evaluated and tested the Extraclassroom Activity Funds of the School District. The result of our tests disclosed that the following areas were not in compliance with the regulations of the Commissioner of Education.

  Clubs with no Financial Activity

  We noted that eighteen high school clubs (Class of 2018, Music – Orchestra, The Knightly News, The Model United, Tri M Honor Society, Mock Trial, Mathletes, Softball, Boys Track, Co-ed Indoor Track, Girls Track, Boys Varsity Soccer, Girls Varsity Soccer, Girls JV Soccer, Girls JV Tennis, X-Country, North Fork Banks) and one middle school club (Maker Space) had no financial activity during the current fiscal year. State Education Regulations provide that the funds of a discontinued activity shall automatically revert to the account of the general student organization or the student council and shall be expended in accordance with the organization's constitution. The Tri M Honor Society, Mathletes, Girls Track, Girls Varsity Soccer and Girls JV Soccer also had no activity in the prior fiscal year.

  Recommendation

  A determination of the status of the clubs with no financial activity should be made to determine the proper disposition of funds. This will deter all clubs from becoming inactive in future years.

  CORRECTIVE ACTION:
  The Class of 2018 and Model United Nations were closed at the end of the 2019-2020 school year.

  The funds in Mock Trial, Girls Track, Girls Varsity Soccer, Girls JV Soccer and Girls JV Tennis, were transferred to the Student Activity account but the accounts have been left open for possible future use.

  Many clubs and team accounts were inactive for a few reasons:
  1. They only meet seasonally (fall, winter, spring)
  2. School closed in March 2020because of COVID-19
  3. The club was not approved for the 2020-21 school year due to COVID-19 (but may run again in 2021-22

  The balances were left in these accounts for future use when the Team/Club resumes activity.

- **Tests of Transactions**

  As part of our audit of the School District's financial statements, we review, evaluate and test controls with respect to the payroll, purchasing, and cash receipt cycles. Our tests of transactions for the current year indicated the following areas were in need of improvement.

CORRECTIVE ACTION PLAN

Glen Cove City School District, New York

Control Deficiencies

User Access Report

Access rights of users of the accounting software should be limited to correlate with each individual's responsibilities. During our audit, we noted three user permission roles that can create and delete claims checks and create and delete vendor information. There also are two user permission roles, which can create and delete payroll checks and create and delete employee payroll information.

Recommendation

To establish stronger controls, we recommend that full access be given to only one key user with others having limited access only to areas in which they would need to perform their job responsibilities.

CORRECTIVE ACTION:

The assistant Superintendent for Business will review the access rights of users and determine if limiting access to one user is reasonable.

Glen Cove City School District, New York

Other Matters

- **Information Technology**

Disaster Recovery/Contingency Planning

The School District does not have well-defined, written disaster recovery procedures and the plan does not extend to the balance of the School District's Information Technology (IT) infrastructure. The time to make contingency plans is before disaster strikes, so that all personnel will be aware of their responsibilities in the event of an emergency situation that precludes the use of the existing IT facilities.

Recommendation

We suggest that management develop a disaster recovery plan covering the entire IT system infrastructure that includes, but is not limited to, the following matters:

- Location of, and access to, off-site storage
- A listing of all data files that would have to be obtained from the off-site storage location
- Identification of a back-up location (name and telephone number) with similar or compatible equipment for emergency processing (management should make arrangements for such back-up with another company, a computer vendor, or a service center; the agreement should be in writing) and subsequently establish procedures to periodically test the back-up files to ensure the data recovery is complete and retrievable as planned.
- Detail procedures to be followed to rebuild individual servers
- Responsibilities of various personnel in an emergency
- Priority of critical applications and reporting requirements during the emergency period
- Climate controlled environments for the server/network rooms.

CORRECTIVE ACTIONS:

The District is using Stafford Associates has the backup site for the District. All data files that would be needed in an emergency are available on the off-site server. The District has a contract with Stafford Associates and will start periodical test of the back-up files in 2021. Detailed procedures to be followed to rebuild individual servers is in progress. The IT Director is working on a list of personnel that would be required to work at the offsite location. He is also working on compiling a list of applications and reporting requirements during an emergency period. The Stafford Associates location is a climate-controlled environment.

- **Cybersecurity Best Practices**

The Government Finance Officers Association ("GFOA") recently published an article entitled "*A Byte of Prevention: Best Practices in Cybersecurity*" to help guide local municipalities in implementing simple, inexpensive and effective strategies that address people, processes and technology to protect organizations from potentially costly and damaging cybersecurity threats. As stewards of sensitive public data, municipal officials and finance officers must understand the significance of this threat, including the large costs governments face in recovering lost data, restoring public trust and recovering from a breach. Most of these ten "best practices" recommendations address the weakest link in cybersecurity – the human factor.

Glen Cove City School District, New York

Other Matters

1. Employee Awareness – Train employees to:
   - Be suspicious of emails asking to change a username or password
   - Double check the sender's email address before opening attachments or links
   - Periodically check the website haveibeenpwned.com to see if their e-mail addresses and passwords have been exposed. If so, employees should report the breach and change passwords for the accounts listed
   - Follow the government's compliance processes when vendors request changes to payment and bank account information (e.g., accounts payable) and staff members (e.g., direct deposit). These are often "out-of-band" (i.e., not done by e-mail) and are therefore vulnerable
2. Patch Digital Devices – Software patches typically include security updates and fixes for vulnerabilities
   - Ensure that all devices (computers, laptops and smart devices) are updated
   - Do not allow personal devices on government networks
3. Anti-Virus Software
   - Install anti-virus software on all devices and run a full scan at least monthly
   - Update anti-virus software regularly
   - Scan mobile devices before they connect to the network
4. Virtual Private Network (VPN) – Encrypts data and sends it through an established tunnel that can only be accessed from an encrypted key at both ends
   - Give all remote workers VPN access.
   - Don't use unsecured public wireless networks if you can help it. If you can't, use VPN, which can be set up by your IT administrators or outsourced to third parties
5. Password Security
   - Develop a policy for strong passwords (i.e. one capital letter, a number, a symbol and a minimum length)
   - Require changing of passwords at set intervals (i.e. monthly/quarterly)
   - Train employees about safe social media practices
6. Administrative Access Controls
   - Implement multi-factor authentication for all administrator accounts (network as well as cloud)
   - Limit the number of administrator (or even super user) accounts as much as possible
7. Physical Security
   - Activate time-out functions so the session logs out after a certain amount of inactive time
   - Activate biometric security (finger print readers/facial recognition software) where feasible
   - Actively manage laptops and smart devices so the information can be erased if device is lost or stolen
   - Use anti-theft software on mobile devices.
8. Back-Up and Disaster Recovery – Preferably at offsite locations separate from your operating network
   - Develop back-up and disaster recovery procedures
   - Ensure that all sensitive data are encrypted.
9. Policies and Procedures
   - Develop policies and procedures that address the use of technology and safe handling of data

Glen Cove City School District, New York

Other Matters

- Procedures should include 1) what staff members are expected to do as "first responders", 2) what the "incident response team" members should do and 3) the communications your public information office should make
- Conduct regular exercises to prepare for responding to cyber threats, which should be part of regular disaster recovery training

10. Consider Cyber Insurance – Generally covers costs associated with hardware replacement, professional services, protecting third parties and cyber ransom
    - Check with your insurance provider about cyber insurance offerings
    - Consider a cyber-security risk assessment (which PKF O'Connor Davies specialists can assist you with)

The full article can be found at https://www.gfoa.org/byte-prevention-best-practices-cybersecurity

In response to addressing best practices in cybersecurity, the District is always looking at new ways to enhance its cybersecurity. The IT Director has addressed the following best practices.

1. Employee Awareness – the District uses GCN training to make employees aware of suspicious emails and websites that are malicious in nature.
2. Patch Digital Devices – our IT department ensures that all devices have updated security and no personal devices are on the school network.
3. Anti-Virus Software – is installed on all devices and updated regularly.
4. Virtual Private Network – access to the VPN is given to few employees as a security measure.
5. Password Security – strong passwords are recommended and all users are required to change their password periodically when the system prompts them to.
6. Administrative Access Controls – the District does not have multi-factor authentication, however the number of administrator accounts are limited as much as possible.
7. Physical Setting – district computers do not have a time-out function or biometric security software. It does have antitheft software on mobile devices and has the software that manages laptops and smart devices so information can be erased if a device is lost or stolen.
8. Back-up and Disaster Recovery – the District has an off-site location in case of an emergency. The IT Director is in the process of developing disaster recovery procedures.
9. Policies and Procedures – The IT Director is working on putting procedures in writing so that all staff members know what to do in case of a cyber-attack.
10. Cyber Insurance – The District has cyber insurance through NYSIR.