Pearl River School District

Report on Internal Controls Pertaining to the Information Technology Cycle

July 2020

Table of Contents

Scope of Engagement

Pursuant to the request of the Pearl River School District and in accordance with the District's December 2019 Risk Assessment Update, we have reviewed the policies, procedures, and internal controls pertaining to the District's Information Technology Cycle.

The objective of our analysis was to determine whether the internal controls pertaining to information systems procedures are adequate and that duties are properly performed thus safeguarding the District's assets.

Work Performed

Our analysis consisted of the following:

1. Examined the following documents made available by the Information Technology Department:

    a) Organizational chart of the Information Technology Department.
    b) District policies pertaining to information technology.
    c) District-Wide Information Technology Plan.
    d) Information technology budgets and current operating costs for the fiscal years 2016/2017, 2017/2018, and 2018/2019.

e) Detailed payment history reports generated by WinCap for the fiscal year 2018/2019 and the period of July 2019 through April 2020.
f) Service Level Agreement entered between the District and Lower Hudson Regional Information Center ("LHRIC") dated July 1, 2017.
g) Inventory schedules of District software.
h) Sample firewall activity report for May 20, 2020.
i) Sample internet filtering log for May 26-27, 2020.
j) Network Topography.
k) List of information technology equipment allowed by District staff to take off school property.
l) Back up and restoration procedures.
m) Restore Job Summary Report dated May 3, 2020.

2. Interviewed the Assistant Superintendent for Business and Director of Information Technology involved in the Information Technology Cycle. During our meetings, we had the opportunity to review documents and direct inquiries regarding transactional records, supporting documents, and timely reporting. The purpose of these interviews was to obtain knowledge as to each individual's job duties and involvement as they pertain to the information systems process, day-to-day responsibilities, who they report to and who they supervise.

3. Assessed possible improvements pertaining to the internal controls of the Information Technology Cycle. Such recommendations are presented within each applicable report section.

Assessment of Information Technology Procedures

The District's current information technology procedures are structured around five (5) distinct categories. We have analyzed each categorical procedure during the course of our audit. We have documented the information systems process by way of narratives for each categorical procedure within Exhibits 1 through 7. For ease of reference, the categories are listed below:

- ***General Controls and Governance***
- ***Software Security Procedures***
- ***Network Security Procedures***
- ***Physical Security Procedures***
- ***Service Continuity Procedures***

General Controls and Governance *(Exhibit 1 through 3)*

The attached Exhibits 1 through 3 summarize the governance procedures of the information technology cycle. Based on our analysis of the information technology governance procedures we have made the following observations and recommendations:

Observation/Recommendation #1

Although the District is performing procedures as documented within the enclosed narratives (See Exhibits 1 through 7), the District should develop formal guidelines regarding software and hardware acquisition, software security, network security, physical security, and service continuity. Current information technology procedures are carried out based on past practices and verbal guidelines provided by the Director of Information Technology.

- ***The District should develop formal documented guidelines and procedures regarding software and hardware acquisition, software security, network security, physical security and service continuity. The documented procedures should be reviewed and updated annually to maintain relevance and reflect regular changes in the information technology environment. The narratives attached to this report should serve as supplemental enclosures to the District's documented procedures.***

The following table summarizes the District's information technology infrastructure and the processes currently carried out by each Administrator/Department:

Administrator/Department	Description
Board of Education	Adopts District Policies and Budget.
Superintendent of Schools	Reviews proposed District Policies and budgetary expenses related to information technology.
Assistant Superintendent for Human Resources & Community Services	Prepares/reviews information technology policies for compliance with regulation.
Assistant Superintendent for Curriculum & Instruction	Assists in coordinating information technology initiatives for instructional purposes that address the needs of the District.
Assistant Superintendent for Business	Prepares/reviews information technology budget to meet current District needs. Assists in coordinating information technology initiatives for business operations that address the needs of the District.
Director of Information Technology	Develops and monitors information technology budget as it relates to District needs and manages related third-party agreements. Manages, prioritizes, and assigns work orders/service tickets based on necessity and complexity. Responsible for project planning, implementation, and systems administration for the District's network and hardware/software. Coordinates the instructional and business needs of the District with the Assistant Superintendent for Curriculum & Instruction and Assistant Superintendent for Business, respectively. Mentor Instructional Technology Coaches. Supervises the Information Technology Department.
LHRIC BOCES	Maintains network infrastructure and network security and resolves high-level issues. Assists in budget development by acquiring quotes and communicating with vendors regarding product specifications. Facilitates project planning, implementation, and systems administration for the District's network and hardware/software. Monitors the District's network access for issues/threats and works to mitigate when necessary.
BOCES Network Specialists (2)	Manages and prioritizes work orders/service tickets based on necessity and complexity. Maintains network infrastructure and network security and resolves hardware/software issues. Assists in project planning, implementation, and systems administration for the District's network and hardware/software. Troubleshoot/resolve user account and workstation issues. Assist on all major rollouts/projects handled by the Information Technology Department.
Part-time Data Specialist	Manages user access to eSchool. Maintains the data stored in the system and creates reports for Administrators to review. Uploads Level 0 and Level 1 student reports to NYSED.
Instructional Technology Coaches (2)	Work with Teachers during technology related professional development. Identify instructional technology needs and assist in planning and coordinating technology initiatives. Train teachers and students how to properly use instructional related software/hardware.

The District has developed a three (3) year technology plan indicating the District's long-term plan of information technology projects.

We conducted a comparative analysis and noted a variance of $153,770, or 9.48%, between the budgetary and actual information technology related expenditures for the fiscal year 2018/2019 as follows:

Account	Description	Initial Budget	Expenditures	Variance	
00-2630-220-000	TECHNOLOGY EQUIPMENT	40,000	800	**(39,200)**	*-98.00%*
00-2630-450-000	TECHNOLOGY SUPPLIES	40,000	10,025	**(29,975)**	*-74.94%*
08-2630-490-000	HIGH COMP ED BOCES SER	460,000	433,760	**(26,240)**	*-5.70%*
30-2630-150-000	MIDL COMP ED CERT SAL	117,445	93,956	**(23,489)**	*-20.00%*
30-2630-490-000	MIDL COMP ED BOCES SER	260,000	250,952	**(9,048)**	*-3.48%*
08-2630-409-000	HIGH COMP ED OTHER EXP	5,000	-	**(5,000)**	*-100.00%*
04-2630-490-000	LINC COMP ED BOCES SER	100,000	95,648	**(4,352)**	*-4.35%*
02-2630-490-000	EVNS COMP ED BOCES SER	100,000	95,648	**(4,352)**	*-4.35%*
03-2630-490-000	FRNK COMP ED BOCES SER	100,000	95,648	**(4,352)**	*-4.35%*
00-2630-460-000	TECHNOLOGY SOFTWARE	7,300	3,051	**(4,249)**	*-58.21%*
08-2630-167-000	HIGH COMP ED N/C SK SB	15,000	11,338	**(3,662)**	*-24.41%*
08-2630-165-000	HIGH COMP ED OT COMP LB	3,000	-	**(3,000)**	*-100.00%*
02-2630-450-000	EVNS COMP ED OTHER SUP	5,000	2,149	**(2,851)**	*-57.02%*
00-2630-160-000	TECHNOLOGY NON INSTRT SAL	95,469	92,716	**(2,753)**	*-2.88%*
03-2630-450-000	FRNK COMP ED OTHER SUP	5,000	2,366	**(2,634)**	*-52.68%*
04-2630-450-000	LINC COMP ED OTHER SUP	5,000	2,648	**(2,352)**	*-47.04%*
08-2630-460-000	HIGH COMP ED SOFTWARE	13,333	12,315	**(1,018)**	*-7.63%*
02-2630-460-000	EVNS COMP ED SOFTWARE	500	-	**(500)**	*-100.00%*
03-2630-460-000	FRNK COMP ED SOFTWARE	500	-	**(500)**	*-100.00%*
04-2630-460-000	LINC COMP ED SOFTWARE	500	-	**(500)**	*-100.00%*
00-2630-402-000	TECHNOLOGY MILEAGE	250	-	**(250)**	*-100.00%*
00-2630-407-000	DIST COMP ED MEMBERSHIP	500	336	**(164)**	*-32.80%*
00-2630-404-000	TECHNOLOGY STAFF DEV	150	-	**(150)**	*-100.00%*
08-2630-160-000	HIGH COMP ED N/C SAL	19,392	19,420	**28**	*0.14%*
30-2630-460-000	MIDL COMP ED SOFTWARE	-	292	**292**	*100.00%*
08-2630-401-000	HIGH COMP ED XEROX/PRNTER	-	415	**415**	*100.00%*
08-2630-220-000	HIGH COMP ED EQUIPMENT	-	1,039	**1,039**	*100.00%*
30-2630-220-000	MIDL COMP ED EQUIPMENT	-	1,175	**1,175**	*100.00%*
00-2630-490-000	TECHNOLOGY BOCES SERV	210,000	213,154	**3,154**	*1.50%*
30-2630-450-000	MIDL COMP ED OTHER SUP	8,000	13,181	**5,181**	*64.77%*
08-2630-450-000	HIGH COMP ED OTHER SUP	10,500	16,037	**5,537**	*52.73%*
Total		**1,621,839**	**1,468,070**	**(153,770)**	*-9.48%*

The Information Technology Department and the LHRIC conduct testing procedures prior to purchasing hardware to determine whether the items will operate in conformity with the design specifications of the District's server and meet the instructional or administrative user requirements.

- ***No recommendations at this time.***

Software Security Procedures (*Exhibit 4)*

The attached Exhibit 4 summarizes the software security procedures of the Information Technology Cycle. Based on our analysis of the software security procedures we have made the following observations and recommendations:

The Information Technology Department tests the software prior to deployment to verify that the software complies with the District's network configuration. The Information Technology Department conducts backup procedures of the original files prior to installing the new software.

The Information Technology Department deploys the software and/or updates onto the server and grants access to specific employee types and students.

The Information Technology Department plans to maintain an approved list of software to install on the Districts network and computers. The Information Technology Department has restricted user rights and does not allow the user to install personal software.

- ***No recommendations at this time.***

Network Security Procedures (*Exhibit 5)*

The attached Exhibit 5 summarizes the network security procedures of the Information Technology Cycle. Based on our analysis of the network security procedures we have made the following observations and recommendations:

The Information Technology Department through the LHRIC has installed a firewall system to prevent intruders from accessing the District's network, an intrusion detection system to prevent unauthorized users from accessing the network, and antivirus software to protect the District's network and computers from malware.

The LHRIC reviews the activity logs recorded in the firewall system when the system reports reduced network connectivity and maintains daily updates of the antivirus software. The LHRIC notifies the District's Information Technology Department if any actions need to take place by the onsite network specialists.

Observation/Recommendation #2

The Information Technology Department has not conducted penetration tests to identify potential vulnerability within the District's network. The lack of penetration tests is a risk as the Information Technology Department may not be aware of the existence of security weaknesses.

- ***The District should consider having a qualified vendor conduct penetration tests to assess the ability to circumvent security features of the system and exploit vulnerabilities to gain unauthorized access. This is an effective way for the District to identify the real-time risks to a network security environment.***

Physical Security Procedures *(Exhibit 6)*

The attached Exhibit 6 summarizes the physical security procedures of the Information Technology Cycle. Based on our analysis of the physical security procedures we have made the following observations and recommendations:

It was indicated that the District has installed air conditioning units and a fire extinguisher in District server rooms to protect the servers from fire and environmental hazards.

Observation/Recommendation #3

Although an employee from the Information Technology Department escorts and supervises all applicable visitors and vendors to the District servers, the Information Technology Department does not maintain an entrance access log nor does it utilize video cameras or otherwise monitor access to any of the building level server rooms and wire closets.

- ***The Information Technology Department should develop an entrance log to the server rooms indicating the individuals, date, entrance, and exit. Documenting the entrance and exit of individuals separate from the Information Technology Department staff will increase the controls over monitoring the access to the District's network/server rooms. In addition, the District should consider deploying video cameras to monitor the site as well as alarms to increase security measures.***

Service Continuity Procedures *(Exhibit 7)*

The attached Exhibit 7 summarizes the service continuity procedures of the Information Technology Cycle. Based upon our analysis of the service continuity procedures we have made the following observations and recommendations:

Observation/Recommendation #4

The District relies on the LHRIC data disaster recovery plan for its critical applications and related data as it subscribes to its backup and data restoration services. The Information Technology Department has not developed a formal documented disaster recovery plan in respect to the District's active directory indicating the alternative processing procedures in the event of loss or interruption of the information technology function.

- ***The District should consider developing a Disaster Recovery Plan to include its current backup and restoration procedures and the current stakeholders responsible to carry out the plan. Based on our analysis of the current plan we recommend including the following:***

  - ***Information pertaining to the backup and recovery programs for books and records that encompass both hard copy and electronic data.***
  - ***Identification and backup of mission-critical systems.***
  - ***Assessment and consideration of financial and operational risks.***
  - ***Definition of alternative communication options between employees and the organization.***
  - ***Establishment of alternative physical locations for employees, with special attention initially to employees who staff the organization's immediate offsite information systems recovery team(s).***
  - ***Impacts on critical constituents, external clients, government agencies, and other relevant organizations in the event of a disruption of continual processing or service.***

- ***Continuation of mandated legislated regulatory reporting in the event of a disruption of continual processing or service.***
- ***Established authorization and access rights to copies of the disaster recovery plan distributed to users.***

The Information Technology Department should test the disaster recovery plan on an annual basis to ensure it works as intended and that users know their duties during a disaster. The testing results should be documented and formally communicated to the Superintendent of Schools.

Observation/Recommendation #5

The Information Technology Department has not scheduled a full interruption test of the District's data backup to be conducted by the LHRIC and LHRIC's restoration procedures, to ensure that the system will perform as intended and that users know how to carry out their duties in the event of a disaster. The LHRIC evaluates the backups of the District's applications and data on a weekly basis.

- ***The Information Technology Department should work with the LHRIC to develop a testing schedule of restoration procedures of the District's data backup for each critical application hosted at the LHRIC. Each backup restoration test should be performed on an annual basis to ensure that the restoration process works as intended and that the Business Office as well as other Departments are able to recover data and perform functions, if needed. The District employees and Internal Auditors should participate during the restoration procedures. The testing results should be documented and communicated to the Information Technology Director, Assistant Superintendent for Business, Assistant Superintendent for Human Resources, and Assistant Superintendent for Curriculum & Instruction for review.***

Risk Rating and Opinion

Inherent Risk Rating: High

Control Risk Rating: Moderate (Pearl River School District)

Audit Opinion: The District's control environment pertaining to the Information Technology Cycle needs improvement. The recommendations noted above are aimed to improve the effectiveness of the information systems process controls within the Information Technology Department.

Exhibits

Exhibit 1 Flowchart of Information Technology Organizational Structure

Exhibit 2 Analysis of Information Technology Policies

Exhibit 3 Narratives of Information Technology General Controls and Governance

Exhibit 4 Narratives of Information Technology Software Security Procedures

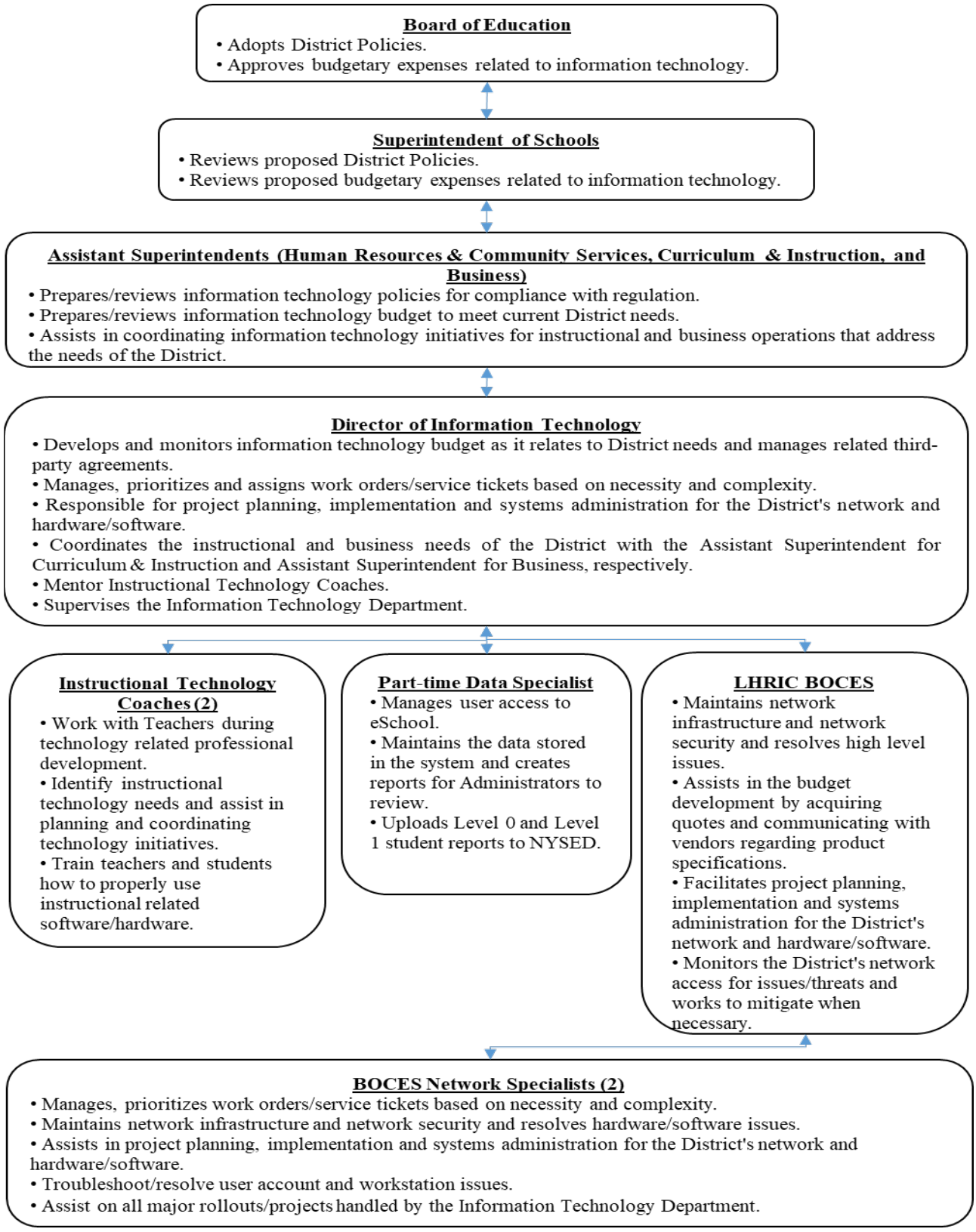
Exhibit 5 Narratives of Information Technology Network Security Procedures

Exhibit 6 Narratives of Information Technology Physical Security Procedures

Exhibit 7 Narratives of Information Technology Service Continuity Procedures

Please contact our Melville, New York office @ 631-756-9500 if you should have any questions in this regard.

Pearl River School District
Report on Internal Controls Pertaining to Information Technology Cycle
Flowchart of Information Technology Organizational Structure
Exhibit 1



The Board of Education adopted on December 12, 1995 Policy 4526 regarding computer use in instruction. According to the policy, the Board of Education is committed to optimizing student learning and teaching. The Board considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in district classrooms solely for the purpose of advancing and promoting learning and teaching.

The Superintendent of Schools shall establish regulations governing the use and security of the district's computer network. All users of the district's computer network and equipment shall comply with those regulations. The Superintendent of Schools shall designate a computer network coordinator to oversee the use of district computer resources. The computer coordinator will prepare in-service programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent, working in conjunction with the Assistant Superintendent for Curriculum and Instruction, the designated purchasing agent for the district, the computer network coordinator and the Curriculum Advisory Council, will be responsible for the purchase and distribution of computer software and hardware throughout district schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

Applicable procedures are documented within the Narratives of Information Technology General Controls (Exhibit 3)

According to the District's Technology Acceptable Use Agreement, the District provides network technology access, including Internet, to all faculty staff and students to enhance the educational mission and instructional goals of the District. In accordance with the NYS Learning Standards for Mathematics, Science, and Technology, students will use technology as a resource to access, generate, process, and transfer information.

A signed user agreement must be on file with the Building Principal, in order to initiate and maintain student use of the District technology network. A breach of this agreement may be considered an act of insubordination, which may result in discipline under the student code of conduct and pursuant to law.

Internet and telecommunications access is provided through the District network. The use of this Internet service is solely in support of school-based research, instruction, and curricula. The District Internet, in compliance with federal law, is filtered at all access points. Any attempt to disable this filtering is a violation of the agreement.

Applicable procedures are documented within the Narratives of Information Technology Software and Network Security Procedures (Exhibits 4 & 5)

The Board of Education adopted on May 14, 2014, Policy 4527 regarding personal computer and mobile device. According to the policy, the Board of Education recognizes that there are personal electronic devices that have educational applications including, but not limited to, tablets, e-readers, calculators, voice recorders, digital cameras and music listening devices. In some instances, a "smart phone" may include applications that permit these functions.

The District provides students and teachers with the computing resources needed to complete technology-related projects. Students and teachers who choose to bring a computer or mobile device of their own to school to use in class or make it more convenient to work on a project both in school and outside of school must comply with District policy.

Students and staff agree to follow the District's Acceptable Use Policy (AUP) when using their own computers and mobile devices in school buildings and on district property. Staff, students, and other users of their own computers and mobile devices agree to abide by all regulations and expectations for appropriate use applying to District technology.

In compliance with the Children's Internet Protection Act (CIPA), the District will use technology protection measures (i.e., internet filtering) to assist in preventing users from accessing inappropriate information on the internet. The District reserves the right to log internet and email use and to monitor file server utilization by users of the District network. The District reserves the right to inspect a personal device should there be a reason to suspect that a user has violated the District's Acceptable Use Policy.

Applicable procedures are documented within the Narratives of Information Technology Software and Network Security Procedures (Exhibits 4 & 5)

The Board of Education adopted on August 7, 2007 Policy 9595 regarding employee computer, network, internet and email use. According to the policy, the District provides computers/devices, networks, Internet access, and/or e-mail to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

All of the District's computers/devices, networks, Internet services, and/or e-mail remain under the control, custody and supervision of the school district. The school district reserves the right to monitor all computer/devices, network, Internet and/or e-mail activity by employees. Employees have no expectation of privacy in their use of school computers/devices. Such monitoring may extend to periodic audits by representatives of the New York State Comptroller's office.

Each employee authorized to access the school district's computers/devices, networks, Internet services and/or e-mail is required to sign an acknowledgment form stating that they have read this policy and the accompanying rules. The acknowledgment form will be retained in the employee's personnel file.

Any employee who violates this policy and/or any rules governing use of the school district's computers/devices, networks, Internet services, and/or e-mail will be subject to disciplinary action, up to and including discharge subject to applicable due process rights. Illegal uses of the school district's computers/devices, networks, Internet services, and/or e-mail will also result in referral to law enforcement authorities.

Applicable procedures are documented within the Narratives of Information Technology General Controls and Governance, Software Security, and Network Security Procedures (Exhibits 3, 4, and 5)

The Board of Education adopted on June 19, 2018 Policy 9596 regarding electronic communication and social media. According to the policy, the Board of Education believes that technology can serve as a powerful tool to enhance education, communication, and learning. Electronic communication, including the use of social media can provide both educational and professional benefits, and prepare students to succeed in their educational and career endeavors. The District is committed to ensuring that all

stakeholders who utilize electronic communication for professional and educational purposes, including staff and students, do so in a safe and responsible manner.

All communication between District staff, students and parents must be done using District email accounts, District approved platforms and/or through a District furnished list of student email addresses and mobile phone numbers compiled through parent consent each school year. This policy and related regulations outline practices for professional/educational electronic communication between District employees as well as between District employees and students.

The District Code of Conduct sets forth expected standards of behavior with respect to student communication, including, but not limited to electronic communication. The Code of Conduct establishes the range of disciplinary options and interventions that can be applied when students engage in misconduct involving electronic communication and social media.

Applicable procedures are documented within the Narratives of Information Technology General Controls and Governance, Software Security, and Network Security Procedures (Exhibits 3, 4, and 5)

Organization's Roles and Responsibilities

- The Information Technology Department is comprised as follows:
  - The **Assistant Superintendent for Human Resources & Community Services** prepares and reviews information technology policies to ensure compliance with regulation.
  - The **Assistant Superintendent for Curriculum & Instruction** assists in coordinating information technology initiatives for instructional purposes.
  - The **Assistant Superintendent for Business** prepares and reviews the information technology budget to meet the current needs of the District. The Assistant Superintendent for Business assists in coordinating information technology initiatives as they relate to business operations within the District.
  - The **Director of Information Technology** is responsible for developing and monitoring the District's information technology budget and managing related third-party agreements. The Director of Information Technology is responsible for project planning, implementation, and systems administration for the District's network and software/hardware. The Director of Information Technology coordinates instructional and business initiatives with the Assistant Superintendent for Curriculum & Instruction and Assistant Superintendent for Business, respectively. The Director of Information Technology supervises the Information Technology Department and mentors the Instructional Technology Coaches.
  - The **LHRIC BOCES ("LHRIC")** is responsible for maintaining the District's network infrastructure and security and resolving high-level issues. The LHRIC assists the District's in the purchasing process by acquiring quotes and communicating with vendors. The LHRIC assists the Director of Information Technology with the project planning, implementation, and systems administration for the District's network and software/hardware. The LHRIC monitors the District's network access and addresses any issues/threats, when deemed necessary.
  - The **BOCES Network Specialists (2)** manage the technical work orders/service tickets. They maintain the District's network infrastructure and network security and resolve hardware/software issues. The BOCES Network Specialists assist the Director of Information Technology with the project planning, implementation, and systems administration for the District's network and software/hardware. The BOCES Network Specialists troubleshoot/resolve user account access, workstation issues, and assist on major rollouts/projects.
  - The **Data Specialist (Part-Time)** manages the eSchool student data management system. The Data Specialist maintains the data stored in eSchool and creates reports for Administrators. The Data Specialist uploads Level 0 and Level 1 student reports to NYSED.
  - The **Instructional Technology Coaches (2)** work with the Teachers and prepare technology related professional development courses. The Instructional Technology Coaches identify instructional technology needs and assist the Director of Information Technology with the planning, coordinating, and implementation of technology initiatives. The Instructional Technology Coaches train teachers and students on the use of instructional software/hardware.

- On July 1, 2017, the District has entered into a service level agreement with the Lower Hudson Reginal Information Center (LHRIC), to provide the Information Technology related management and technical services through the combination of shared on-site staff and a Managed IT (MIT) Lead. According to the agreement, LHRIC provides the following services:

  - Management services including project management, problem solution and troubleshooting, consulting vendor resource management, and technology support.
  - Technical services including support for district owned client devices and peripherals.
  - Systems services including support and management of servers, storage devices, and virtual solutions.
  - Wireless services including support and management of the local wireless solution.

- The LHRIC is subject to annual audits of its data protection procedures to verify that they comply with the service organization contract (SOC) 2 security and privacy principles and criteria.

Long-Term Planning

- The District has developed a three (3) year information technology plan indicating the District's long-term plan of information technology projects. The most recent update of the District's technology plan was developed for the fiscal years 2018 through 2021. The District's information technology plan includes the following sections:

  - Mission and Vision
  - History
  - 2018-2021 Technology Goal Focus
  - Emerging Technologies
  - Technology Coordination/Oversight
  - Professional Development
  - Instructional Integration of Technology Resources
  - Educators as Technology Facilitators
  - District Technology Assessment-Infrastructure Components
    - Network
    - Devices
    - Applications
    - Data
  - Goals and Strategies
  - Budgeting

Short-Term Planning

- Short-term planning is carried out to make specific plans to implement short-term tasks that may be important and urgent. Based on the District's needs and fiscal year budgets, the Information Technology Department determines the priority of tasks as well as the fiscal year budget.

Budget and Operating Costs

- The budget process is initiated by requests submitted by the building level Teachers and Administrators for their instructional technology needs. Their requests are reviewed by the Director of Information

Technology, the Assistant Superintendent of Curriculum & Instruction, and the Assistant Superintendent of Business prior and during the budget season and is documented within the District's budget notes. The Director of Information Technology assesses whether the requested equipment could be purchased through a five (5) year Installment Purchase Agreement (IPA) through LHRIC. In general, the Districts information technology budget includes the following expenses:

- Salaries
- Equipment
- LHRIC/BOCES Services
- Software
- Supplies

Software Acquisition and Management

- Principals contact the Information Technology Department to request a purchase of new software or informational resource databases.

- The vendors provide the Information Technology Department with the information pertaining to the parameters, capabilities, and requirements of the system and software products.

- The Assistant Superintendent of Curriculum & Instruction in conjunction with the Director of Information Technology review and approve the major program initiatives. If the program involves new technology, the Information Technology Department reviews the technical aspects of the software and determines whether the software is compatible with the District's network environment.

- The Information Technology Department reviews the LHRIC contracts for the requested software. If the items are not included in the LHRIC contracts, the Information Technology Department obtains quotations from the vendor and ensures that the District receives the best price, in accordance with the District's purchasing policies and guidelines.

- Upon review, the Information Technology Department forwards the requisition order to the Superintendent of Schools and Assistant Superintendent of Business for approval. Upon approval, the requisition is converted to a purchase order.

- If deemed necessary, the Information Technology Department engages an outside vendor or the LHRIC to provide training services for the use of the software application.

- The Information Technology Department maintains and updates annually a list of approved purchased software and licenses, including the servers and/or workstations the software is installed on.

Hardware Acquisition and Management

- Prior to the procurement of hardware, the Information Technology Department evaluates the usage, tasks, and requirements for the equipment and the environment in which the equipment will be used. Among the factors to be evaluated are:

    - Information processing requirements such as major existing application systems and future application systems and workload and performance requirements.

  - Hardware requirements such as central processing unit (CPU) speed, disk space requirements, memory requirements, peripheral devices, direct entry devices, networking capability, and the number of terminals needed to support the system.

- The Information Technology Department and the LHRIC conduct testing procedures prior to purchasing hardware to determine whether the items will operate in conformity with the design specifications of the District's server and meet the instructional or administrative user requirements.

In general, the District purchases the following Information Technology hardware:

Vendor	**Description**
Dell	Workstations, Chromebooks
Apple	iPads
HP	Printers
Toshiba	Phones

The District utilizes the following software:

Operating Systems:

Windows 7.0 Enterprise
Apple iOS 10
Chrome OS 66.0.3359.137

Office Management/Administrative Software

Microsoft Office	Frontline-IEP	WinCap
Adobe	MyLearningPlan	Transfinder
eSchoolData	Smart Notebook	Aesop

Instructional & Curriculum Software/Research Database

Achieve 3000 - informational text resource	Letter Writer	MS Picture Viewer	SS Test Maker
Adobe Design Suite	Inspiration	Neighborhood Map Machine	Text Bridge Pro
Autocad Suite	Math Arena	Pasco Data Studio	The Graph Club
Bailey's Book House	MATH Test Generator	PyschSim	Time Liner
Geometer Sketchpad	Mavis Beacon	Renaissance Learning - Accelerated Math	Tux Paint
Google Earth	Mavis Instructor	Renaissance Learning - STAR Reading Assessment	Type to learn Network
Google for Education	Micro Type Pro	Renaissance Learning -STAR Math Assessment	Understanding Math
Impact Online	Millie' Math House	SCIENCE Exam View	West Point Bridge Designer
Inspiration	MS Office	SCIENCE Test Maker	
IrFanView	MS Paint	SMART	
Kidspiration	MS Photo Story	Social Studies Test Maker	

- The Information Technology Department tests the software prior to deployment to verify that the software complies with the District's network configuration. Depending on the software, the Information Technology Department conducts back up procedures of the original files prior to installing the new software.

- The BOCES Network Specialist deploys the new software and/or updates on the District's network and disseminates to each computer.

WinCap

- Through Citrix, the Information Technology Department has implemented a virtual desktop infrastructure in respect to WinCap which gives users the ability to access the software from other workstations within the District that have internet access through a secure and encrypted connection.

Network Security Software

- The Information Technology Department, through the LHRIC, utilizes the following Network Security Software:

Network Security Software	Purpose
Lightspeed/Cisco	Monitor web activity
Cisco	Manage Firewall
Sophos	Manage Anti-Virus
Cisco	Detect intrusions to the system
Lightspeed	Filter spam from email messages

- The Information Technology Department monitors the network security software alerts and reviews the exemptions listed on the activity logs.

- The Information Technology Department maintains regular updates of the server and operating system to ensure efficient performance and adequate security to ongoing changes and threats.

- The Information Technology Department does not maintain open network ports on the servers. The District's network does not allow dial-in capabilities, gateways to and from the network that the Information Technology Department does not administer, workstations or servers with internal or external modems, wireless routers, or other telecommunication devices that enable inbound or outbound access. The Information Technology Department allows VPN access only to the BOCES Network Specialists.

- The Information Technology Department utilizes wireless access District-wide. Wireless access points at the building level are protected via password to serve the District's network from unauthorized users and prevent them from accessing the network data. The District allows wireless internet access to guests through a network separate from the one utilized by District staff and/or students. The guest network is subject to the District's web-filtering provisions.

The District has not conducted a penetration test to identify any vulnerability within the District's network.

- The Information Technology Department grants access for a limited period to vendors to conduct their support services for specific projects such as upgrades on virtual machines and the District's network. These vendors are given temporary credentials that are revoked after the need for them has elapsed. They assign access to the specific machine for a limited period.

Server Rooms/ Main Distribution Frames

- The Information Technology Department maintains eighteen (18) servers at the High School and several switches at each school and the Administration Building. The High School serves as the District's Main Distribution Frame. A network schematic is included within the District's Technology Plan.

Although visitors are escorted or supervised by an employee from the Information Technology Department, the District does not maintain a log of the individuals accessing the Server Room at the High School.

- The server room has air conditioning units installed to maintain a constant temperature.

- The Information Technology Department has plugged all equipment in the server room to surge protectors to protect the servers from spikes in power surges. In addition, the Information Technology Department utilizes an uninterrupted power supply (UPS) to power the servers when normal utilities are not available.

Portable Equipment

- The District allows certain Administrators, Teachers, and Students to take Chromebooks, Laptops, iPads, and Cameras off school property to perform their respective job duties and assignments. In accordance with the District's Acceptable Use Policy, these individuals, are required to sign an agreement form indicating their acknowledgment of the District's security policy and their responsibility of any physical damages or theft of the loan equipment. The Information Technology Department maintains a list of employees and students who have been provided with information technology equipment.

- The LHRIC performs repair services on information technology equipment.

Active Directory/Emails/WinCap

- The Information Technology Department performs daily backup snapshots of the District's active directory, emails, and financial application WinCap. The snapshots are incrementally stored on the District servers and are replicated at the LHRIC. The LHRIC maintains the following backups:

  - Up to two (2) months of daily incremental backups are maintained on disk.
  - Eleven (11) monthly full backups are maintained on tape.
  - One (1) annual backup is maintained on tape and forwarded to an offsite location at Iron Mountain, NY, which is kept for seven (7) years.

- The Information Technology Department has developed controls whereby the financial application WinCap is hosted at the LHRIC and users are connected through a secure FTP Channel to perform their duties and record transactions. The LHRIC performs daily offsite backups of the WinCap database at Harrison, Iron Mountain, and West Nyack, NY.

- The LHRIC performs test and restoration procedures on a monthly basis of application data hosted at the LHRIC servers. During the restoration procedures, the LHRIC validates the data, evaluates the results, and ensures that the data are successfully restored onto their network. The monthly test and restoration procedures are performed on a random basis and are not specific to any district. Successful validation of these tests is a validation for all districts that participate in the LHRIC's remote backup service.

E-School

- The student data management system, eSchool, is a web-based application that is hosted and backed up by the LHRIC within its servers.

Disaster Recovery Plan

- The District relies on the LHRIC data disaster recovery plan for its critical applications and related data as it subscribes to its backup and data restoration services.

Pearl River School District

Ann Marie Tromer
Assistant Superintendent for Business
135 West Crooked Hill Road
Pearl River, New York 10965-2730
TromerA@pearlriver.org
Phone: 845-620-3999

October 2, 2020

Darin V. Iacobelli
Nawrocki Smith LLP
290 Broad Hollow Road, Suite 115E
Melville, NY 11747

Dear Darin:

The Pearl River School District (the 'District') has received the report titled "Pearl River School District, Report on Internal Controls Pertaining to the Information Technology Cycle, July 2020."

The Pearl River School District hereby submits below a Corrective Action Plan for the Report on Internal Controls Pertaining to the Information Technology Cycle which is required under Section 170.12 of the Regulations of the Commissioner of Education.

Recommendation #1:
The District should develop formal documented guidelines and procedures regarding software and hardware acquisition, software security, network security, physical security and service continuity. The documented procedures should be reviewed and updated annually to maintain relevance and reflect regular changes in the information technology environment. The narratives attached to this report should serve as supplemental enclosures to the District's documented procedures.

District Response: The District will work with the Director of Information Technology to develop any additional guidelines needed as discovered as a result of this review.

Recommendation #2:
The District should consider having a qualified vendor conduct penetration tests to assess the ability to circumvent security features of the system and exploit vulnerabilities to gain unauthorized access. This is an effective way for the District to identify the real-time risks to a network security environment.

District Response: The District has noted the recommendation and will work with the LHRIC to preform penetration tests.

Recommendation #3:

Although an employee from the Information Technology Department escorts and supervises all applicable visitors and vendors to the District servers, the Information Technology Department does not maintain an entrance access log nor does it utilize video cameras or otherwise monitor access to any of the building. The Information Technology Department should develop an entrance log to the server rooms indicating the individuals, date, entrance, and exit. Documenting the entrance and exit of individuals separate from the Information Technology Department staff will increase the controls over monitoring the access to the District's network/server rooms. In addition, the District should consider deploying video cameras to monitor the site as well as alarms to increase security measures.

District Response: The District has noted the recommendation and respectfully feels that the fact that all server rooms are locked and only opened when supervised by an IT Department escort is sufficient protection. We agree that cameras would be extra security, but installation of cameras is currently a budgetary constraint.

Recommendation #4

The District should consider developing a Disaster Recovery Plan to include its current backup and restoration procedures and the current stakeholders responsible to carry out the plan.

District Response: The District has noted the recommendation and will work with the LHRIC to create a Disaster Recovery Plan based on Cyber Security and Infrastructure Security Agency recommendations.

Recommendation #5

The Information Technology Department should work with the LHRIC to develop a testing schedule of restoration procedures of the District's data backup for each critical application hosted at the LHRIC. Each backup restoration test should be performed on an annual basis to ensure that the restoration process works as intended and that the Business Office as well as other Departments are able to recover data and perform functions, if needed. The District employees and Internal Auditors should participate during the restoration procedures. The testing results should be documented and communicated to the Information Technology Director, Assistant Superintendent for Business, Assistant Superintendent for Human Resources, and Assistant Superintendent for Curriculum & Instruction for review.

District Response: The District has noted the recommendation and will work with the LHRIC to develop a testing schedule of restoration procedures.

Thank you.

Ann Marie Tromer