GOVERNANCE

Policies and Procedures

The District is responsible for maintaining compliance with Education Law §2-d and the Family Educational Rights and Privacy Act ("FERPA") which provide clear protections for student data. The District has adopted a comprehensive set of formal Board policies relating to information technology as required by the New York State School Boards Association. The *District Technology Plan* discusses the District's plans for instructional technology, hardware, software, implementation, and infrastructure inventory. The plan specifically covers District policies related to data backup, hardware and equipment, email, network accounts, network security, wireless access, and software.

Insurance

Cyber and privacy liability exposure is a growing risk for governmental entities. Data breach trends include hacking, lost or stolen laptops, backup tape loss, staff mistakes, and vendor and business partner breaches. Data breach incidents may be both accidental and intentional. The costs related to governmental cyber and privacy breaches can be extreme. Some of these costs may include crisis service costs, legal costs, and replacement costs. As a result, cybersecurity insurance is becoming increasingly popular among governmental entities. Cybersecurity insurance could reduce the number of cyber-attacks by promoting the adoption of preventative measures for increased protection and encouraging best practices. The District currently has a cybersecurity insurance policy with New York Schools Insurance Reciprocal.

Information Technology Services Contracts

The District contracts with Nassau Board of Educational Services ("BOCES") for some of its information technology services. As part of their agreement with the District, Nassau BOCES provides services including but not limited to curricular support software and training as well as support and maintenance of the special education student management system, *IEP Direct*. The District utilizes *PowerSchool* for student data management. This application allows the District to track attendance, behavior, grades, and scheduling by student. The system assists the District in preparing required reports submitted to the New York State Education Department. PowerSchool is a web–based system that allows teachers, administrators, instructional clerical staff, and counselors to access student information. System administration is provided by the vendor. The District has contracted with several assessment and classroom management applications including *Apple School Manager, Naviance,* and *Schoolnet*. These applications are used as plug-ins in conjunction with *PowerSchool*. In addition, cloud backup services for the District's accounting and student information systems are provided based on the District's contract with *CSDNET*.

Disaster Recovery Plan

The District has developed a *Disaster Recovery Plan* that includes procedures related to preparing for recovery or continuation of technology infrastructure critical to the District after a disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications, such as networking, and other information technology infrastructure.

While districts would like to ensure zero data loss and zero time loss in the event of a disaster, the cost associated with that level of protection may make the desired high availability solutions impractical. The primary goal of the District's Plan is to restore operations quickly and with the most current data available. Under the Plan, additional objectives include but are not limited to the following:

- Developing an orderly course of action for restoring critical computing capability;
- Making the decision to recover at a cold site or repair the affected site;
- Developing an organizational structure to carry out the plan; and
- Identifying the equipment, floor plan, procedures, and other items necessary for recovery

NETWORK AND NETWORK SECURITY

Firewalls and Intrusion Detection Systems

A firewall is used to implement access control between two networks. It allows the District's network users to access outside information while preventing those outside the District from accessing the District's systems. The network engineer and firewall engineer are responsible for monitoring and managing the firewall including performing all updates and configurations. All firewall events and activities are logged and the logs are reviewed daily by the network engineer, firewall engineer and cybersecurity group for suspicious activity. Alerts of suspicious activity are sent via email to the network engineer and firewall engineer.

An intrusion detection system ("IDS") is a device or software application that monitors a network or systems for malicious activity or policy violations. The system blocks or drops traffic in response to a suspicious event identified by the IDS. The IDS sends alerts of suspicious activity to the network engineer and information technology staff. In addition, IDS logs are reviewed daily by the network engineer. The District provides an added layer of security for District email through the use of *Barracuda,* an email security product.

Physical Security

The District's Network Operations Center ("NOC"), is located at the High School. The NOC and other *Main Distribution Frames* ("MDFs"), located at each of the other District locations, are the primary network locations that house approximately 30 physical servers and 80 virtual servers. Additionally, there are 33 *Intermediate Distribution Frames* ("IDFs") throughout the District. All server rooms are physically secured and have uninterrupted power supply ("UPS") units in place to protect the District's equipment from an unexpected power disruption that could cause business disruption or data loss. MDFs and IDFs are also temperature controlled.

Backup Controls

The District performs local and remote backups of the accounting information system, student information system, email server, and administrative and teacher data. The District has two network centers which data is backed up to, as well as to an off-site location at the Middle School Network Operations Center. Backups are stored to a hard drive, storage area network, and/or tapes. Tapes are secured in a fireproof safe located in the business office. As an additional measure, the District stores backups to a secure offsite facility for critical data such as its student information system and accounting information system. In addition to the multi-layered approach to backups,

the District has other provisions in place to reduce the risk of ransomware data corruption. Since ransomware and data corruption are sometimes not discovered until after backups have been overwritten, the District has implemented a semi-annual procedure to airgap the backup tapes. An airgap is a security measured that creates an impenetrable barrier between a digital asset and malicious actors, such as a virus, hacker, power surge or any force that threatens a digital asset. It ensures total isolation of a given system electromagnetically, electronically, and physically from other networks, especially those that are not secure.

Network and Email Access

Microsoft Exchange provides the District's email service and the District uses Active Directory synchronization for the authentication of email and network users. The Deputy Superintendent and Network Engineer are responsible for system administration. A *Personal Action Report* is completed for new employees who require access to the District's network and other applications. The new employee's information is completed by the human resources department and the information technology department completes the technology related section of the *Personal Action Report,* which indicates all user access required to be granted to new employees. When new teachers are hired, they are required to complete information technology training, which includes a review of the District's best practices for security. New employees must complete a *Computer, Network, and Internet Use Agreement Authorization form* as a formal acknowledgement of the *District Computer, Network, and Internet Use Policy.* Existing employees receive a copy of this policy on an annual basis. Similarly, students and parents must review the *District Computer, Network, and Internet Use Policy* and complete a related authorization form stating the user will comply with the requirements outlined in the policy. Other efforts to increase information technology security awareness include the presence of a footer on all incoming emails originating outside the District which cautions users to beware of potentially harmful emails and to contact the information technology department with any questions.

Remote Access

Remote access for systems maintenance to the District's network is granted by the Deputy Superintendent and/or Network Engineer in the Information Technology Department. Remote access is granted (when needed) utilizing a secure VPN connection via the Sonicwall Firewall (Generation 7 Firewall). VPN traffic is highly secure and encrypted end to end. The VPN connection is closely monitored by the Network Engineer and disabled when no longer needed. All users have the ability to access their virtual desktop through a secure connection server and email and *PowerSchool* can be access through the District's website, from any location, utilizing their related login credentials.

Passwords

Access to computerized files and transactions should be restricted to authorized individuals only. This can be accomplished through the use of passwords and software that restricts user access to help ensure that only authorized individuals utilize the computer system. *Active Directory* network user passwords consist of a minimum of eight characters and must meet complexity requirements (at least one of each character type: uppercase, lowercase, numeric, and symbolic). Users are required to change their passwords every 90 days and new passwords cannot be the same as the last twenty-four passwords for that user. The District's administrative network policy is set to lockout users after six invalid login attempts and will timeout after being idle for thirty minutes.

STUDENT DATA SECURITY

Student Information System Access

Access to the District's student information system, *PowerSchool*, is granted to employees utilizing the same process as network access and linked using LDAP to their Active Directory network credentials.

Users can access their *PowerSchool* account while on the District's network as well as externally through the District's website. Passwords for District employees are held to the same complexity level as Active Directory and in conformance to our policy.

Users must change their password every ninety days. The District enforces a lockout policy for *PowerSchool* based on IP address rather than individual user accounts. This policy is set at fifteen failed login attempts and will prevent additional attempts from that IP address until it is reset by a system administrator. Access to personally identifiable information in *PowerSchool* over an internet connection is encrypted by a transport layer security ("TLS") or secure sockets layer ("SSL") configuration and full perfect secrecy. Users in *PowerSchool* are assigned to a security group based on their job description. Restrictions are applied to individuals' user privileges within *PowerSchool* to ensure that only authorized users are permitted to view specific information.

IEP Direct Access

IEP Direct is the special education student management system currently utilized by the District. *IEP Direct* is a web-based application, hosted by Nassau BOCES, that is used to track student Individualized Education Programs ("IEPs"), evaluations, and meetings, and assists with the preparation of New York State required reports including System to Track and Account for Student ("STAC") forms. *IEP Direct* also facilitates District compliance with applicable privacy laws and regulations. Access to *IEP Direct* is granted by the Director of Special Education. Requests for access are originated by the Assistant Director of Special Education, who emails *Frontline* to request a new account. Access is only available to individuals to perform their job functions. Additionally, access is restricted within the system to be consistent with job responsibilities.

Data Breach – Sensitive Personally Identifiable Information ("PII")

A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. District PII is stored in *PowerSchool, IEP Direct, Transfinder,* and *Nutrikids*. PII is also accessed by Nassau BOCES and through plug-ins in *PowerSchool*. The District does not allow third party access to the PII data with the exception of the application vendor. District employees are instructed to use encryption when transmitting PII data. The District utilizes a variety of methods including DropBox, Fax, or a vendor's secure transmission portal (similar to the one we used to send the auditors confidential information for this audit). The District has also adopted Board policy No. 8635, Information Security Breach and Notification, which identifies the need to secure private information and procedures to be followed in the event of a breach. The District is not aware of any incidents of data breach of their PII data.

ACCOUNTING INFORMATION SYSTEM

The District utilizes *Wincap* as its accounting information system ("AIS"). This application was installed by the vendor and requires application updates, database management and, if necessary, system restores. The District performs a variety of functions within the accounting information system including but not limited to budget development, accounting, requisitions, receivables, and payroll. Access to *Wincap* must be initiated by the Deputy Superintendent or Supervisor of Teaching, Learning, & Assessments in conjunction with the Assistant Superintendent for Business.

Permissions and Passwords

A good internal control framework requires District management to develop a system of controls that includes proper segregation of duties in the District's operations, not only in manual processes, but also within the AIS. *Wincap* allows the system administrator to restrict access to functions specific to job descriptions. Passwords for *Wincap* are required to be a minimum of eight characters long and must meet complexity requirements (at least one of each character type: uppercase, lowercase, numeric, and symbolic). Users are required to change their passwords every 90 days and new passwords cannot be the same as any previous password for that user. The District also enforces a lockout policy for its AIS, which will lockout after six failed attempts.

FINDINGS AND RECOMMENDATIONS

Based on our interviews, observations, and detailed testing, we have provided our findings and recommendations below to further strengthen the District's internal controls as they pertain to information technology outlined above.

It should be noted that these recommendations are provided to the District to assist management in improving the District's internal controls and procedures relating to information technology. It is important to note that our findings and recommendations are directed toward the improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

***

Policies and Procedures

Procedure Performed: We reviewed the District's policies and procedures with regard to the internal controls related to information technology.

Finding: No exceptions were found as a result of applying these procedures.

***

Information Technology Services Contracts/Parents' Bill of Rights

Procedures Performed: We reviewed the District's Parents' Bill of Rights to ensure compliance with Education Law §2-d and the information technology services contracts for six third party vendors who collect personally identifiable information.

Findings: No exceptions were found as a result of applying these procedures.

***

Required Annual Notifications

Procedures Performed: We reviewed the District's annual notifications required under the Family Educational Rights and Privacy Act ("FERPA") for the required elements.

Findings: No exceptions were found as a result of applying these procedures.

***

Server Rooms

Procedures Performed: We physically inspected the District's MDFs located at the High School and Middle School as well as an IDF located at the Middle School to verify the server rooms are properly secured, monitored, and that the servers are reasonably protected from fire and floods. We also inquired of the other network facilities located throughout the District.

Finding: No exceptions were found as a result of applying these procedures.

***

Permissions/Access Controls

Procedure Performed: We reviewed the access controls surrounding the District's network, accounting information system, student information system, and special education student management system.

Finding: No exceptions were noted as a result of applying these procedures.

***

Procedure Performed: We reviewed the user permissions within the student information system and special education student management system to identify possible permissions granted to employees that may not be consistent with their job responsibilities.

Finding: No exceptions were noted as a result of applying these procedures.

***

Procedure Performed: We reviewed the user permissions within *Wincap* to identify possible permissions granted to employees that may not be consistent with their job responsibilities.

Finding: No exceptions were noted as a result of applying these procedures.

***

Procedure Performed: We reviewed user accounts for the District's network, student information system, and special education student management system to identify multiple active user accounts, generic user accounts, and ensure individual accounts are associated with current, active District employees.

Finding: No exceptions were found as a result of applying these procedures.

***

Disaster Recovery Plan

Procedure Performed: We reviewed the District's Disaster Recovery Plan (the "Plan") to determine that the Plan identifies critical information technology infrastructure and equipment, establishes the most suitable recovery strategy for each application utilized by the District, and identifies those individuals responsible for overseeing the disaster recovery process.

Finding: No exceptions were found as a result of applying these procedures.

***

CORRECTIVE ACTION PLAN

The District is required to prepare a corrective action plan in response to any findings contained in the internal audit reports. As per Commissioner's Regulations §170.12, a corrective action plan, which has been approved by the Board, should be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be submitted using the NYSED Business Portal.