Hicksville Union Free School District
Report on the Internal Controls of the Cybersecurity Cycle
June 2018

Table of Contents

I. Scope of Engagement

The Board of Education of Hicksville Union Free School District has engaged Nawrocki Smith, LLP to provide internal audit services with respect to the District's policies, procedures, and internal controls pertaining to the Cybersecurity Cycle. As part of this engagement, we performed extensive analysis and validation tests within the District's Cybersecurity Cycle.

The objective of our analysis was to determine whether the internal controls pertaining to cybersecurity are adequate, to ensure that duties are properly performed and that the controls over information systems are implemented and that assets are properly safeguarded. In order to verify that the cybersecurity area has proper internal controls, we interviewed key personnel and tested various transactions to ensure the key controls within these areas are operating effectively.

Our analysis within each functional area consisted of the following:

- Documented functional area policies and procedures applicable to the Cybersecurity Cycle after interviews and discussions with key employees.
- Identified key controls within each functional area of the Cybersecurity Cycle and performed audit tests of those controls.
- Made observations and recommendations pertaining to the internal controls of the Cybersecurity Cycle based upon observations and testing that was performed.

Interviews and inquiries were conducted with the following District employees:

Title	Department
Director of Educational Technology & Grants	Information Technology Department
Information Technology Consultant	Information Technology Department

II. General Controls and Governance

Policies and Procedures

The Hicksville Union Free School District has an Information Technology (IT) Department that consists of the Director, four (4) technicians and an outside consultant. All Information Technology Department staff report to the Director of Educational Technology & Grants. The Director is responsible for managing and maintaining security surrounding the District's networks, software programs, and technology assets.

The District adopted Policy #4526 *Internet/Network Use* in April 2013 which outlines the acceptable uses of the District's network and internet, blocking and filtering to be installed, required monitoring of use, and training of staff and students to be provided.

Observation and Recommendation #1 **Risk Rating: Moderate**

We noted that the District has not adopted an Information Security Breach and Notification Policy which should address identifying confidential information including student data, employees responsible for checking for breaches, how often inspection is to be performed and the employee to be notified in the event of such breach. This policy is required by State Technology Law §208.

- *We recommend that the District consider developing the above mentioned policy to ensure that procedures in place are formally documented and to ensure that incidents are resolved consistently.*

Observation and Recommendation #2 **Risk Rating: Low**

It was noted that the District has not developed a formal computer controls procedure which should address segregation of duties, passwords and permissions, remote access, schedule of data backups and backup restoration testing, etc. However, it should be noted that procedures are in place that cover these areas and some of these procedures are in the process of being revised.

- *We recommend that the District consider developing a computer controls procedure to formally document the procedures currently in place. A strong procedure defines appropriate segregation of duties, password policies that are consistent for all users, schedules and documentation for backups and restoration testing, protocol for granting permissions and remote access, etc.*

Inventory

The Information Technology Department maintains inventory listings in Excel to track and monitor IT related equipment. Deliveries of technology equipment are maintained within the Technology Department and included in the inventory before distribution throughout the District.

We randomly selected thirty (30) assets from the Information Technology Department's inventory report and performed a physical inspection of each asset comparing the location, type, make, model, and serial number to the inventory listing.

Observation and Recommendation #3 **Risk Rating: Low**

We noted that there were three (3) assets included in the inventory listing that were marked for disposal and one (1) inventory item in use that could not be located. In addition, we noted the asset tag for two (2) items did not match the inventory listing.

- *We recommend that the Information Technology Department perform an observation to identify equipment that is in use by the District but not included in the inventory report. This will ensure that the technology inventory report is accurate.*

III. Education and Training

Threats are always evolving in the cyber environment and it is essential that all users are educated about the types of threats and proper responses to those threats to ensure the ongoing security of the District's data. The District ensures that security measures are followed and that all staff and students are aware of potential cybersecurity threats through ongoing education and training.

Policy #4526 *Internet/Network Use* requires the District to provide training on the Internet Safety Policy to staff and students at the beginning of each school year. We noted that the Director of Technology & Grants provided training to all staff at the 2017/2018 Superintendent's Conference. In addition, all IT Department staff receive ongoing training.

- *No recommendation at this time.*

IV. Access Rights

Access to the District's network and applications is granted after a request has been reviewed and approved by the IT Department. Changes to an employee's access rights requires approval from their direct supervisor and the IT Department. Passwords must be reset after a set amount of days and the characters in the password must meet the District requirements.

We reviewed the listing of all users with an active account for Active Directory, District email, and IEP Direct. We compared the reports to the personnel listing to determine that all users were active employees or consultants of the District.

Observation and Recommendation #4 **Risk Rating: Low**

We noted that the District does not require users to sign an acceptable use agreement before access is granted to the network. An acceptable use agreement documents that the user understands and will comply with the terms related to use of District equipment.

We also noted that the District's applications contained active accounts for employees that were no longer with the District as follows:

- Active Directory – one hundred and twenty nine (129) accounts
- District email – one hundred and fifty eight (158) accounts
- IEP Direct – thirty (30) accounts

- *We recommend that the District develop a standard Acceptable Use Agreement for all users to sign before access to the network is granted. Only those users who have signed the agreement should be granted access to the system. The agreement should address staff and student responsibility, access to the system, district liability, system security, privacy, etc. This procedure may be incorporated into the hiring process. In addition, all users should sign an agreement each year to renew access. The District may consider an electronic agreement that could be automated with the log-in process.*

- *The District should also consider developing a standard procedure for the Human Resource Department and/or Business Office to notify the Information Technology Department of user accounts that must be deactivated as a result of termination of employment, completion of a contract or other separation from the District. This will also provide formal documentation of changes and enhance the controls over the active directory.*

Remote Access

Remote access allows communication with the District's network from a remote location or facility. Currently, only three (3) individuals have remote access through a District assigned laptop.

- *No recommendation at this time.*

V. Vulnerability & Privacy and Protection of Data

The District utilizes an internet filter to monitor computers and restrict internet access as appropriate for staff and students. The Network is protected by a firewall that is monitored by the Information Technology Department. The firewall is set up to block unauthorized access while permitting other authorized access and communications.

We have contracted with BMB Consulting, Inc. to perform vulnerability testing as part of our internal audit of the Cybersecurity Cycle. The District is in the process of upgrading their firewall and requested that the test be performed on the new system. A separate report detailing the results of the vulnerability testing will be issued in the 2018/2019 school year.

VI. Incident Reporting and Response

Incidents are reported through the IT e-ticket system. IT Department staff will review the report and determine the appropriate response. Responses are also documented in the e-ticket system. Any emergency situations are communicated directly to the Director of Educational Technology and Grants.

We reviewed log of e-tickets submitted from January 1, 2018 to April 30, 2018 and noted all tickets within the service type "cybersecurity," six (6) in total, were resolved timely and responses were documented in the notes to the ticket.

- *No recommendation at this time.*

VII. Risk Rating and Audit Opinion

Inherent Risk:	High
Control Risk:	Low
Audit Opinion:	Satisfactory

RISK RATING DEFINITIONS

Inherent Risk – Inherent risk is the risk of a material misstatement in the un-audited information assuming the absence of internal control procedures. Inherent risk includes any risk arising from fraud. As with other risks, inherent risk may be evaluated at various levels of aggregation (e.g. financial statement level, account balance assertion level) and at various stages during the course of the audit (e.g. client acceptance/retention state, audit planning stage, etc.).

> **Inherent *Risk*** *is particular to the area being reviewed if there were no controls in place. Thus, if there were no control procedures in place pertaining to the particular area, what is the risk of a material misstatement.*

Control Risk – Control risk is the risk that a material misstatement in the un-audited information will not be detected and corrected by management's internal control procedures on a timely basis. Auditors evaluate control risk at the account balance assertion level based on a detailed knowledge of the client's business. Auditors may evaluate this risk in the second, third, and forth audit stages, namely the audit planning, control testing, and substantive testing stages.

> **Control Risk** *is particular to the District's controls currently in place in the area being reviewed. Thus, what is the risk of a material misstatement with the control procedures currently in place.*

Audit Opinion – Based upon the audit work performed and our assessment of the controls within each particular audit area an audit opinion is provided for each audit area from one of the following three (3) categories:

Satisfactory:	Controls are operating effectively
Needs Improvement:	Controls need improvement for effectiveness
Unsatisfactory:	Controls are unacceptable and need immediate improvement

Hicksville Union Free School District
Cybersecurity Narrative – Exhibit A
June 2018

The following is a narrative, or a sequence of events, which describes the various functions within the Cybersecurity Cycle of the Hicksville Union Free School District. The narrative was derived from discussions and interviews with key IT Department employees as well as observations of controls within the District. The cybersecurity function has been broken down by area for ease of reference, including the following areas:

I. General Controls and Governance
II. Education and Training
III. Access Rights
IV. Vulnerability
V. Privacy and Protection of Data
VI. Incident Reporting and Response

Blue = Internal Control

I. General Controls and Governance

- The Hicksville Union Free School District IT Department is responsible for cybersecurity and the protection of data.
- The IT Department consists of the Director of Educational Technology & Grants, four (4) technicians, and a secretary.
- The District also hired an outside Consultant to assist the IT Department. The four (4) technicians report to the Consultant.
- The following Board of Education approved policies, with adoption or amendment dates, are currently in place regarding protection of data:
    - *#1240 The Public's Right to Know, March 1983*
    - *#4321.5 Confidentiality and Access to Individualized Education Programs, Individualized Education Services Programs and Service Plans, August 2016*
    - *#4526 Internet/Network Use, April 2013*
    - *#4526.1R Internet Safety Regulation, August 2015*
    - *#5311 Student Rights and Responsibilities, December 1996*
    - *#5500 Student Records, January 1987*
- The District has standard forms that employees sign to acknowledge their responsibility for using the District's network.
- The following services are provided by third party administrators:
    - Power School – the District's student record management software
    - IEP Direct – the District's special education record management software
    - Nvision – the District's financial application
- The District has contracts with vendors to provide services for web filtering, anti-virus protection, firewalls, etc.

II. Education and Training

- New teachers receive training on the use of certain programs in new teacher orientation at the beginning of the school year. New teachers coming in mid-year do not receive the same level of training.

- Other new employees will receive one-on-one training from the Director of Educational Technology & Grants when hired.
- **The Director of Educational Technology & Grants provided training to all staff at the Superintendent's Conference for the 2017/2018 school year. This training covered the District's IT policies and procedures as well as awareness for email scams and virus detection.**
- Some of the District's purchased applications come with IT support. The IT Department becomes more familiar with the products through contact with IT support when addressing any questions or issues.
- **The IT Department also holds formal training for IT staff. Sign in sheets are maintained to track attendance**.

III. Access Rights

- Access to the District's applications is requested through the IT e-ticket system.
- **When a request is received to grant access to a new employee, the IT Department will contact the Human Resources Department to confirm that the individual was hired. The IT Department will also review the Board of Education minutes to verify.**
- Substitute teachers are not given network accounts.
- **Changes to employee's access rights are granted after approval is received from their direct supervisor and the IT Department.**
- **Active Directory passwords reset every thirty (30) days.** Passwords must be at least eight (8) characters and contain an upper case letter, a lower case letter, a number, and a special character.
- **Password resets are not sent through inter-office email. Instead, the employee must come to the IT office to get a new password or a new password will be sent to a Lexmark printer in their building. Lexmark printers can only be accessed using an ID badge.**
- Student passwords are stored by the IT Department, but the employee passwords are not.
- Password requirements for Power School are the same as the District's, however the user ID is different from Active Directory.
- Remote access to the District's network is granted to the Assistant Superintendent for Business, the High School Principal and the Middle School Principal.
- These individuals sign an acknowledgement letter that was prepared by the District and their attorney, Guercio and Guercio.
- The VPN client is set up on a District laptop and access will only be granted through this laptop.

IV. Vulnerability

- **The District's server is located in a separate room in the Administration building. Access is limited to few employees.**
- **The server room is locked at all times and must be opened with a key. Cameras have been installed to face the door to see who is entering the room. The camera also has a temperature and humidity sensor.**
- Each building has its own virtual local area network ("VLAN") with a subset of internet protocol ("IP") addresses.
- The IT Department can monitor where the user is based on the IP address.
- Wireless access points are on a separate VLAN. The District has four (4) wireless networks. There is a faculty network for District devices, faculty network for personal devices, student network and guest network.
- The faculty network for personal devices only grants internet access.

- The guest network is only available for use after 2:30 pm. The signal strength for access points near windows is turned down to limit the number of users.
- The District also has a separate VLAN for a testing environment. This VLAN has internal access only and cannot access the internet.
- The Power School server has a section for administration and a separate section for teachers, parents and students.
- The administrative server can only be accessed by certain individuals internally. Only the High School and Middle School Principals have VPN access because they maintain the master class schedules.
- Power School VPN access is granted through a secure set of IP ranges.
- There is also an open IP address for parents and students to access Power School from their home.
- Power School technicians are granted remote access to the District's network when tech support is needed. A log in to access the network must be given over the phone each time access is requested.
- Users access Nvision through BOCES. First the user logs into the BOCES server and can then launch Nvision.
- IEP Direct is accessed through a website. There is a link through Power School that creates a secure connection to IEP Direct once logged in.
- The IT Department receives firewall logs, VPN logs, and anti-virus logs to track attempts to access the network.
- Active Directory also has a separate log that tracks user log ins and log outs.

V. Privacy and Protection of Data

- The District's agreements with vendors contain a rider that addresses retention and destruction of data.
- The vendor would be responsible for any breach of the conditions in the contract.
- Sensitive data is protected through various IT procedures. For example, student social security numbers are not stored in Power School. Instead, the school ID number is used as the unique identified. In addition, administrators cannot access other administrator's files on the District network.
- Data sent through email is not encrypted, but the transmission is. The email is sent through a secure tunnel which has a SSL certificate.
- **District data is backed up to tape on a daily, weekly, and monthly basis.**
- **The tapes are maintained in a safe in one of the District's school buildings. The safe is located in a locked room that is designated for this purpose. Only the Director of Educational Technology & Grants, the IT Consultant and the Director of Facilities have access to this room.**
- When equipment is discarded, the hard drives are maintained to protect any data that has been stored.
- Printers leased through Xerox also have hard drives. When the machine is taken away or replaced, the hard drive is given to the District.

VI. Incident Reporting and Response

- Incidents are reported through the IT e-ticket system. The e-ticket system includes the date of the request, request type, and description of the noted issue.
- The IT staff will determine the appropriate response to the specific incident and document that response in the notes to the e-ticket.

- Any emergency reports are communicated directly to the Director of Educational Technology & Grants.
- When the IT Department is notified of any computers that have a potential virus, the computer is isolated on the network.