NawrockiSmith

Northport – East Northport Union Free School District

Report on Internal Controls Pertaining to the Information Technology Cycle

June 2018

Table of Contents

Scope of Engagement

Pursuant to the request of the Northport Union Free School District and in accordance with the District's February 2018 Initial Risk Assessment, 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) District Policies pertaining to information technology.
   b) District Short and/or long-term District-Wide Information Technology Plan(s).
   c) Information Technology budgets and current operating costs.
   d) Payment History Reports generated by NVision for fiscal years ended June 30, 2015, 2016 and 2017.
   e) User permissions report generated by NVision as of May 24, 2018.

f) Employee personnel file report generated by NVision as of May 24, 2018.
g) Log In/Out activity report in respect to the District's network for May 3, 2018.
h) Permission summary in respect to administrative access to the District's Active Directory.
i) Activity reports pertaining to firewall, spam filter, VPN remote access, and internet activity.
j) Copy of penetration test report dated January 2018.
k) Entrance/Exit log to the District's server rooms.
l) Topography of the District network
m) Disaster Recovery Plan dated January 2018
n) Forms utilized by the Information Technology Department

2. Interviewed the Assistant Superintendent for Student Services, Technology & Assessment, Administrator of Technology, and District Senior Systems Engineer 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 eight (8) 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 10. For ease of reference, the categories are listed below:

- ***General Controls and Governance***
- ***Information Technology Fixed Asset Procedures***
- ***Logical Security Procedures***
- ***Data Security Procedures***
- ***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 upon 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 our enclosed narratives (See Exhibits 1 through 12), the District has not developed documented formal guidelines regarding software and hardware acquisition, information technology inventory management, creating and modifying user accounts, data security, software security, network security, physical security, service continuity, social media accounts, and email security. Information Technology procedures are carried out based upon past practices and verbal guidelines provided by prior and current Administrators.

- ***The District should develop documented guidelines and procedures regarding software and hardware acquisition, information technology inventory management, creating and modifying user accounts, data security, software security, network security, physical security, service continuity, social media accounts, and email security. 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 processes currently carried out by each Administrator/Department:

Administrator/Employee	**Description**
Assistant Superintendent for Student Services, Technology & Assessment	Coordinates and supervises the Information Technology Department, develops and manages information technology budget, and manages information technology initiatives, manages leases with BOCES. Oversees information technology department clerical day to day acquiring quotes and ordering supplies.
Administrator of Technology	Responsible for project planning implementation and systems administration for NVision. Oversees data management and reporting to NYSED. Coordinates professional development. Supervises Instructional Technology Resource Teachers, District Senior Systems Engineer, Lead Technicians, and Level 1 Technicians. Oversees information technology department clerical day to day filing and answering phones for the Information Technology Department.
District Senior Systems Engineer	Maintains network infrastructure and network security, and resolves hardware/software issues. Resolves workstation issues.
Lead Technician	Coordinates work orders for desktop troubleshooting.
Level 1 Technicians (5)	Resolve workstation issues.
Instructional Technology Resource Teachers (6)	Responsible for training 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 informational technology projects for the fiscal years 2015 through 2018.

The District's portion of the Smart Schools Bond Act of 2014 is $1,300,000 for which the District has chosen to allocate these funds to address the needs documented within the information technology plan.

Pursuant to the Commissioner's Regulations (Part 100.12), the Information Technology Department develops annual instructional technology plan surveys that compiles data related to the District's technology planning and needs.

We have analyzed the appropriations status report applicable to information technology expenditures for the fiscal years 2014/2015, 2015/2016 and 2016/2017. We noted that information technology expenditures increased by $496,254, or 10.26%, from $4,835,343 in 2014/2015 to $5,331,597 in 2016/2017.

	2014/2015	**2015/2016**	**2016/2017**
Information Technology Expenses	**4,835,343**	**4,986,046**	**5,331,597**
Change From Prior Year	*N/A*	*150,703*	*345,551*
% Change From Prior Year	*N/A*	*3.12%*	*6.93%*

We conducted a comparison analysis and noted a variance of $256,194, or 4.58%, between the budgetary and actual information technology related expenditures for the fiscal year 2016/2017 as follows:

Category	Adj Budget	Expensed	Difference	
BOCES Services	1,817,359	1,653,255	**(164,105)**	*-9.03%*
Computer Software	2,532,666	2,480,665	**(52,001)**	*-2.05%*
Equipment Maintenance/Repair	113,332	96,589	**(16,743)**	*-14.77%*
Educational Supplies	80,733	64,887	**(15,846)**	*-19.63%*
Teacher Aide Salaries-Computer Studies	213,954	208,280	**(5,674)**	*-2.65%*
Telephone Expense	6,600	4,989	**(1,611)**	*-24.41%*
Contract Services	346,166	345,952	**(214)**	*-0.06%*
Instructional Salaries	476,980	476,980	-	*0.00%*
Total	**5,587,790**	**5,331,597**	**(256,194)**	*-4.58%*

➢ ***No recommendations at this time.***

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

➢ ***No recommendations at this time.***

Information Technology Fixed Asset Procedures (Exhibit 4)

The attached Exhibit 4 summarizes the fixed asset procedures of the Information Technology Cycle. Based upon our analysis of the information technology fixed asset procedures we have made the following observations and recommendations:

The Information Technology Department maintains an inventory list within the inventory application "Follett" for information technology assets. Once the assets are delivered at the building level, the Information Technology Senior Typist Clerk updates the inventory with the applicable tag numbers and serial numbers. The Information Technology Department performs building level physical inspections of information technology equipment and also reconnects the equipment to the network during the summers of each year subsequent to the custodians cleaning the rooms. The District is planning to conduct a full inventory of information technology equipment during the Summer of 2018 to ensure the accuracy of the Follett inventory list.

➢ ***No recommendations at this time.***

Logical Security Procedures (Exhibit 5)

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

The Human Resources Department notifies via email the Information Technology Department of new hires, retirements, terminations, and changes in employment status, job titles, and duties.

Based upon the employee's job position and the instructions from the Human Resource Department and the Business Office, the Information Technology Department inputs the employee's information into an

Access database that automatically notifies the District Senior Systems Engineer to grant, change, or inactivate the employee's access to the District's Active Directory, email, Google domain, Noodle, and other applicable applications.

The Assistant Superintendent for Business and the Administrator of Technology are responsible for assigning and reviewing user permissions pertaining to NVision. The District assigns user access based on the employee's job position.

The Information Technology Department has developed controls whereby users are required to change their passwords on a regular basis in the Active Directory and/or NVision.

The Information Technology Department has developed controls whereby a user account is automatically locked after several unsuccessful log-in attempts.

Observation/Recommendation #2

We analyzed the user permission report from NVision and noted that access to the financial application for one (1) former employee was not disabled. We also noted that one District cabinet member had access to perform data entry and setup parameters in the human resource module. Based on limited information provided to date, we were unable, at this time, to determine whether the District's cabinet members have utilized such permissions.

- ***The Information Technology Department should disable the former employee's access to NVision. The Human Resource Department should notify the Information Technology Department of any employee position changes, including new hires, transfers, and terminations.***

  The user permissions should be limited to each employee's job roles and duties. The Business Office and the Information Technology Department should limit the permissions for the Cabinet members to "view only" for their respective departments. This recommendation will assist the District in minimizing the access of NVision to the individuals authorized by the Board of Education.

  The Business Office should periodically review the permissions user account report and verify the appropriateness of user accounts and permissions on an individual employee basis. This recommendation will assist the Business Office in increasing its oversight and controls over its access to the District's accounting system.

Subsequent to our review, the Information Technology Department took immediate corrective action plan and implemented the above recommendations.

Observation/Recommendation #3

The Information Technology Department is in the process of developing controls to automatically lock the screens of the workstations when no activity has occurred.

- ***The Information Technology Department should finalize its logical security controls whereby workstations will automatically lock the screens after a period of inactivity. The Information Technology Department should also require users to log off their account before stepping away from their computers and before they leave for the day. This will ensure that unauthorized users will not access the District's systems and their information.***

Subsequent to our review, the Information Technology Department took immediate corrective action plan and implemented the above recommendations.

Data Security Procedures (Exhibit 6)

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

Access to confidential information is restricted to the respective Administrators and employees, which the District identifies, to prevent unauthorized users view, alter, delete, or steal this information.

The Information Technology Department has established protocols to prevent building level Administrators and Clerical employees from saving data on their personal desktops or laptops. It is current policy that all data is saved on the network.

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

Software Security Procedures (Exhibit 7)

The attached Exhibit 7 summarizes the software security procedures of the Information Technology Cycle. Based upon 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 back up procedures of the original files prior to installing the new software.

The Information Technology Department deploys the software and/or updates onto server and grants access to specific employee types and students. Based on the job position, the users or students access the software through their virtual desktop images.

The Information Technology Department maintains an approved list of software to install on the District's network and computers. The Information Technology Department has restricted the user rights and does not allow the user to install personal software.

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

Network Security Procedures (Exhibit 8)

The attached Exhibit 8 summarizes the network security procedures of the Information Technology Cycle. Based upon our analysis of the network security procedures we have made the following observations and recommendations:

The Information Technology Department has implemented a virtual desktop infrastructure (VDI) in respect to the District's server, which gives users the ability to access their desktops from any workstation as long as they have Internet access. The Information Technology Department has classified the VDI desktop images into three (3) groups for Administrators, Teachers, and Students and has developed controls whereby users only access the District VDI through a secure and encrypted SSL connection.

The Information Technology Department 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 an antivirus software to protect the District's network and computers from malware. The Information Technology Department monitors the network security software alerts and reviews the exceptions listed on the activity logs.

The Information Technology Department has recently conducted penetration tests to identify potential vulnerability within the District's network. The District is planning to continue performing such tests on a semi-annual basis.

➢ ***No recommendations at this time.***

Physical Security Procedures (Exhibit 9)

The attached Exhibit 9 summarizes the physical security procedures of the Information Technology Cycle. Based upon our analysis of the physical security procedures we have made the following observations and recommendations:

The Information Technology Department escorts and supervises all applicable visitors and vendors to the District servers and maintains an entrance log to monitor access to any of the building level server rooms.

The Information Technology Department utilizes an uninterrupted power supply (UPS) to power the servers when normal utilities are not available.

We have conducted a walkthrough observation of the District's server rooms and we verified that the District has installed air conditioning units and fire extinguishers to protect the servers from fire and environmental hazards.

The District allows certain Administrators and Teachers to take laptops or Chromebooks off school property in order to perform their respective job duties. The Information Technology Department requires these employees to sign a release form when they receive District's equipment. The Information Technology Department maintains a list of employees who are authorized to take these laptops.

➢ ***No recommendations at this time.***

Service Continuity Procedures (Exhibit 10)

The attached Exhibit 10 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:

The District's most recent disaster recovery plan was developed in January 2018. The disaster recovery plan is drafted to support the recovery of District's operations within the critical business and academic departments. Based upon our analysis of the draft plan, we noted the plan includes following:

1. Disaster identification and declaration
2. DRP activation
3. Communicating the disaster

4. Assessment of current and prevention of further damage
5. Establish IT operations
6. Repair and rebuilding of primary facility

Observation/Recommendation #4

The District does not store backups of the Active Directory at a secured, off-site location.

- ***The District should consider the cost/benefits of maintaining off-site backup to allow for a restoration of data even if the original data within District premises is destroyed.***

Observation/Recommendation #5

The Information Technology Department has not conducted a full interruption test of its data backup and 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 Information Technology Department should conduct annual full interruption tests of its data backup and restoration procedures to ensure that the restoration process works as intended and that the Business Office is able to recover data, if needed. As an alternative to the above recommendation, the Information Technology Department should develop a testing schedule of restoration procedures for each critical application and perform such at various times on an annual basis to ensure that the restoration process works as intended and that the Business Office is able to recover data, if needed. District employees and Internal Auditors should participate during the restoration procedures. The testing results should be documented and communicated to the Assistant Superintendent for Business for review.***

Risk Rating and Opinion

Inherent Risk Rating:	High
Control Risk Rating:	Low
Audit Opinion:	The District's control environment pertaining to the Information Technology Cycle is satisfactory. The recommendations noted above are aimed to improve the effectiveness of the user permission and data restoration procedures and the related responsibilities and controls within the Business Office and the Information Technology Department.

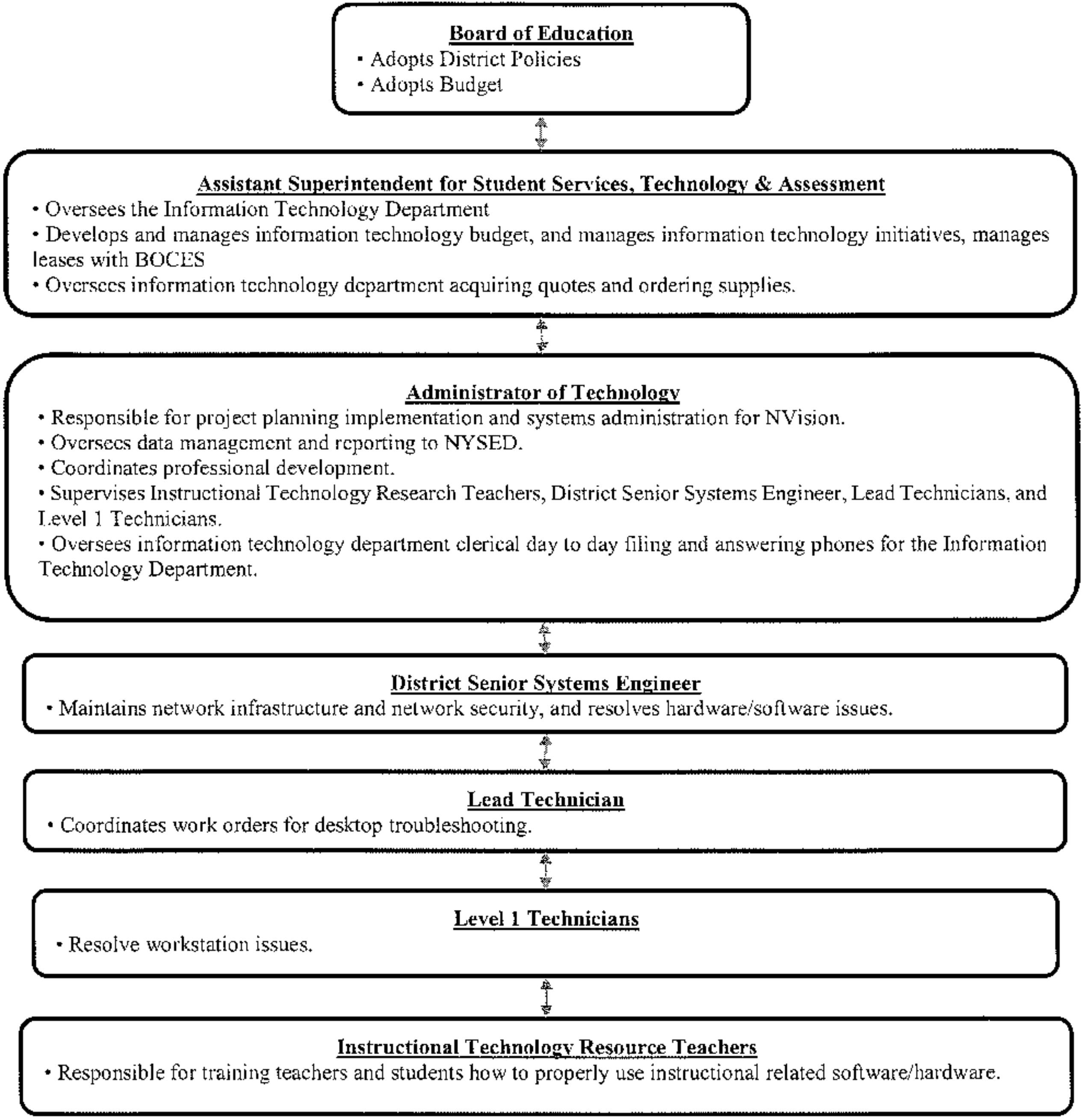
Exhibits

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 Fixed Asset Procedures
Exhibit 5	Narratives of Information Technology Logical Security Procedures

Exhibit 6	Narratives of Information Technology Data Security Procedures
Exhibit 7	Narratives of Information Technology Software Security Procedures
Exhibit 8	Narratives of Information Technology Network Security Procedures
Exhibit 9	Narratives of Information Technology Physical Security Procedures
Exhibit 10	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.

Flowchart of Information Technology Organizational Structure
Exhibit 1



Board of Education
- Adopts District Policies
- Adopts Budget

Assistant Superintendent for Student Services, Technology & Assessment
- Oversees the Information Technology Department
- Develops and manages information technology budget, and manages information technology initiatives, manages leases with BOCES
- Oversees information technology department acquiring quotes and ordering supplies.

Administrator of Technology
- Responsible for project planning implementation and systems administration for NVision.
- Oversees data management and reporting to NYSED.
- Coordinates professional development.
- Supervises Instructional Technology Research Teachers, District Senior Systems Engineer, Lead Technicians, and Level 1 Technicians.
- Oversees information technology department clerical day to day filing and answering phones for the Information Technology Department.

District Senior Systems Engineer
- Maintains network infrastructure and network security, and resolves hardware/software issues.

Lead Technician
- Coordinates work orders for desktop troubleshooting.

Level 1 Technicians
- Resolve workstation issues.

Instructional Technology Resource Teachers
- Responsible for training teachers and students how to properly use instructional related software/hardware.

Analysis of Information Technology Policies
Exhibit 2

The Board of Education adopted on July 7, 2010 Policy 4526 regarding the use of Computer Network for Education. According to the policy, the following rules and regulations govern the use of the district's computer network system and access to the Internet:

I. Administration
The Assistant Superintendent for Instruction and Administration or his / her designee shall:
- Monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- Be responsible for disseminating and interpreting district policy and regulations governing use of the District's network at the building level with all network users.
- Provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- Ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.

II. Internet Access
- Students will be provided access during class time, during the school day when the students are not in class, and before or after school hours as appropriate.
- Students in grades 1 – 12 will be provided with individual accounts. Students in Kindergarten will share
- classroom accounts.
- Students may browse the World Wide Web:
- A staff member will monitor these activities as they do all other educational experiences.

III. Acceptable Use and Conduct
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password.
- Only those network users with written permission from the Assistant Superintendent for Instruction and Administration or his / her designee may access the District's system from off-site (e.g., from home).
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher or administrator.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the District's network.

Applicable procedures are documented within the Narratives of Information Technology General Controls and Governance, Logical Security, Software Security, and Network Security Procedures (Exhibits 3, 5, 7, 8)

The Board of Education adopted on September 13, 2010 Policy 4526.1 regarding the use of Internet Safety. According to the policy, the Superintendent of Schools shall procure and implement the use of technology protection measures that block or filter Internet access by:

- Adults to visual depictions that are obscene or child pornography, and

Analysis of Information Technology Policies
Exhibit 2

- Minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee. The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

Applicable procedures are documented within the Narratives of Information Technology Network Security Procedures (Exhibit 8)

The Board of Education adopted on October 22, 2015 Policy 8630 regarding the use of <u>Computer Resources and Data Management</u>. This policy covers all adult users of computers and other technology that may provide access to the Internet and/or other networks within or linked with the School District. According to the policy, the Superintendent of Schools shall be responsible for designating an individual(s) who will oversee the procurement and use of School District computer resources. Said individual will prepare in-service programs for the training and development of School District staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas. The policy includes rules and regulations regarding the use of the School District's computer network system, email accounts, employee access to the Internet, and management of computerized records.

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

The Board of Education adopted on November 19, 2015 Policy 8635 regarding the use of <u>Information Security Breach and Notification</u>. According to the policy, the Board of Education directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure.
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

The policy includes rules and regulations regarding the procedures identifying security breaches, methods of notification, and notifications to the State and Other Agencies.

Applicable procedures are documented within the Narratives of Information Technology Network Security Procedures (Exhibit 8)

The Board of Education adopted on November 19, 2010 Policy 9225 regarding the use of <u>Acceptable Use Policy for Users</u>. According to the policy, users should have no expectation of privacy when using the school's computers, networks, Internet services, e-mail and other technology. The District retains control, custody and supervision of all computers, networks, Internet and e-mail services owned and leased by

Analysis of Information Technology Policies
Exhibit 2

Northport-East Northport UFSD and reserves the right to monitor all computer and Internet activity by employees and other system users. Network administrators will deem what is inappropriate use and their decisions are final. The network administrators may close a telecommunications account at any time. Users must acknowledge their understanding of this policy as a condition of using a District Internet account or using the network facilities.

Applicable procedures are documented within the Narratives of Information Technology Logical Security, Data Security, Physical Security, and Network Security (Exhibits 5,6,7,8)

Narratives of Information Technology General Controls and Governance
Exhibit 3

Organization's Roles and Responsibilities

- The Information Technology Department is comprised as follows:

  - **Assistant Superintendent for Student Services, Technology & Assessment** coordinates and supervises the Information Technology Department, develops and manages information technology budget, manages information technology initiatives, and manages leases with BOCES. The Assistant Superintendent for Student Services, Technology & Assessment oversees information technology department clerical day to day acquiring quotes and ordering supplies.

  - **Administrator of Technology** is responsible for project planning implementation and systems administration for NVision and for overseeing data management and reporting to NYSED. The Administrator of Technology coordinates professional development and supervises Instructional Technology Research Teachers, District Senior Systems Engineer, Lead Technicians, and Level 1 Technicians. The Administrator of Technology oversees information technology department clerical day to day filing and answering phones for the Information Technology Department.

  - **District Senior Systems Engineer** (Third Party Service Provider No.1) Maintains network infrastructure and network security, and resolves hardware/software issues.

  - **Lead Technician** (Third Party Service Provider No.2) Coordinates work orders for desktop troubleshooting.

  - **Level 1 Technicians (5)** (Third Party Service Provider No.3) Resolve workstation issues.

  - **Instructional Technology Resource Teachers (6)** are responsible for training teachers and students how to properly use instructional related software/hardware.

Long Term Planning

- The Smart Schools Bond Act of 2014 authorized the issuance of $2 billion of general obligation bonds to finance improved educational technology and infrastructure to improve learning and opportunity for students throughout the State. The District's portion of this funding is $1,300,000. The District has developed a three (3) year technology plan indicating the District's long-term plan of informational technology projects. The most recent update of the District's technology plan was developed for the fiscal years 2015 through 2018. The District's technology plan includes the following:

  - Mission and Visions Statements
  - Current and Future Technology Needs
  - Technology Plan
    - Improving Education
    - Assessing Services and Resources
    - Goals, Strategies, and timeframes
  - Professional Development Strategies
  - Community Involvement
  - Evaluation
  - Budget
  - District Policies

Narratives of Information Technology General Controls and Governance
Exhibit 3

Short Term Planning

- Pursuant to the Commissioner's Regulations (Part 100.12), the Information Technology Department develops an annual instructional technology plan survey that compiles data related to the District's technology planning and needs. The Information Technology Department developed its most recent instructional technology plan survey during 2017 and included the following:

    - District Information
    - Instructional Technology Vision and Goals
    - Technology and Infrastructure Inventory
    - Software and IT Support
    - Curriculum and Instruction
    - Professional Development
    - Technology Investment Plan
    - Status of Technology Initiatives and Community Connectivity
    - Instructional Technology Plan Implementation
    - Monitoring and Evaluation

- Short-term planning is carried out to make specific plans to implement short-term tasks that may be important and urgent. Based upon 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 Technology Committee including the Assistant Superintendent for Student Services, Technology & Assessment, Administrator of Technology, Building Administrators, and Instructional Technology Resource Teachers. A secondary review is performed by the District's cabinet members during budget season and is documented within the District's budget notes. In general, the District's information technology budget includes the following expenses:

    - BOCES Services
    - Computer Software
    - Material & Supplies
    - Repairs & Maintenance
    - Professional Development
    - Telecommunication Systems
    - Technicians
    - Warranty Services

Narratives of Information Technology General Controls and Governance
Exhibit 3

Information Resource/Software Acquisition and Management

- Principals and/or the Special Education Department contact the Information Technology Department to request a purchase of informational resources from textbook publishers.

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

- The Information Technology Department reviews and evaluates the technical software specifications and determines whether the software meets the District's instructional or administrative needs.

- The Information Technology Department reviews state and BOCES contracts for the requested software. If the items are not included in any of the contracts, the Information Technology Department obtains quotations from other vendors to ensure 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 Assistant Superintendent for Student Services, Technology & Assessment and the Assistant Superintendent for Business for approval. Upon approval, the requisition is forwarded to the Purchasing Agent to convert the request to a purchase order.

- If deemed necessary, the Information Technology Department will engage the Instructional Technology Resource Teachers to provide training services for the use of the software application. The Information Technology Department maintains a schedule of software training conducted at the District.

- The Information Technology Department maintains a list of approved purchased software and licenses including the servers or workstations the software is installed at.

Hardware Acquisition and Management

- The Information Technology Department schedules major hardware purchase projects during late fall and late spring of each year. Prior to the procurement of hardware, the Information Technology Department conducts surveys with other Districts regarding their experiences with similar hardware purchases. Furthermore, 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 number of terminals needed to support the system.

- The Information Technology Department conducts testing procedures of demonstration units pertaining to major hardware 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. The Information Technology Committee discuss the testing results during their monthly meetings.

Narratives of Information Technology Fixed Asset Procedures
Exhibit 4

- The Information Technology Departments utilizes an inventory software application "Follett Resource Manager" to account for information technology equipment. The inventory application contains the following information:

  Asset Tag
  Model
  Manufacturer
  Cost
  Date Purchased
  Purchase Order Number
  Location
  Warranty

- Suffolk BOCES maintains an inventory of information technology equipment leased by the District. The Information Technology includes the BOCES leased equipment within the "Follett" inventory application.

- Once the assets are delivered at the District's Middle School Warehouse, the Information Technology Department updates the inventory list with the applicable tag and serial numbers. The Information Technology Department also updates the information technology inventory throughout the year to include additions, transfers, and disposals occurred at the building level.

- The Information Technology Department performs building level physical inspections of information technology equipment and also reconnects them to the network during the summers of each year subsequent to the custodians cleaning the rooms. The District is planning to conduct in the Summer of 2018 a full inventory of information technology equipment during the Summer of 2018 to ensure the accuracy of the Follett inventory list. Furthermore, the Information Technology Department requires student laptops and Chromebooks to be returned to their applicable building for inspection, clean up, and repairs. The District's external auditors perform sample physical inspections as part of their audit fieldwork. At the end of each fiscal year, the Information Technology Department performs a walkthrough of obsolete items identified by Suffolk BOCES within their annual "End of Life Information Technology Asset List."

- District employees are required to submit a work order to request repair or troubleshooting services for their workstations or other information technology related equipment. The Information Technology Department has implemented a control whereby a work order cannot be submitted unless the information technology equipment is listed within the "Follett" inventory application.

- Information technology equipment are disposed or excessed upon approval by the Board of Education which is documented within the Board of Education minutes. The Information Technology Department removes and destroys the hard drives from the disposed equipment.

- The Business Office prepares proposals for the community to purchase the obsolete equipment.

Narratives of Information Technology Logical Security Procedures
Exhibit 5

Creating, Modifying, and Deleting User Accounts

- The Human Resources Department notifies via email the Information Technology Department of new hires, retirements, terminations, and changes in employment status, job titles, and duties. Based on the employee's job position, the Assistant Superintendent for Business determines the user's access to modules and account codes within the financial application NVision. The email notifications include employee information, action dates, job positions, and requests and approvals of an employee's logical access to any computerized information including NVision. The Human Resource Department requires new hires to sign off on the "Acceptable Use Policy for Users (Employees, Consultants, Volunteers and Other District Authorized Personnel), Use of District Computers, Networks, Internet Access, and E-Mail System" form indicating their acknowledgment of the District's information technology policies. A copy of the signed form is maintained within the employee's personnel file.

- Based upon the employee's job position and the instructions from the Human Resource Department and the Business Office, the Information Technology Department inputs the employee's information into an Access database that automatically notifies the District Senior Systems Engineer to grant, change, or inactivate the employee's access to the District's Active Directory, email, Google domain, Noodle, and other applicable applications.

- On an annual basis, the Assistant Superintendent for Business reviews the NVision user permission reports and determines the access level and authority for an individual or role with reference to his or her job position. This review process is also performed when a new employee assumes the duties and responsibilities of a former user.

- Upon termination, the Human Resources and Information Technology Departments contact the employee, receives equipment, and removes all access rights from the network. The removal of access rights of former employees includes the following:

  - Physical and logical access
  - Identification (ID) cards
  - Subscriptions
  - Equipment (Laptop/iPad/Chromebooks/Cell Phones/Keys)

  The Information Technology Department maintains a database to ensure all user access has been revoked from the former employee.

Logon ID Requirements

- The logon IDs are restricted to provide individual, but not group, identification. Each user gets a unique logon ID that can be identified by the system. The format of logon IDs is typically standardized and kept confidential.

The Information Technology Department is in the process of developing controls to automatically lock the screen of each workstation if no activity has occurred.

Narratives of Information Technology Logical Security Procedures
Exhibit 5

- The Information Technology Department has developed controls to automatically disconnect a user's session with the server and or application as follows:

Category	Server/Application	Session Expiration
Student	VDI Server/Active Directory	Immediately subsequent to end of class/project 50 minutes of inactivity – student is logged out
Employee	VDI Server/Active Directory	Subsequent to Six (6) Hours of Inactivity – 50 minutes of inactivity, user is disconnected; after 6 hours of inactivity while disconnected, user is logged out
	NVision	Per VDI Parameters - Subsequent to Six (6) Hours of Inactivity – 50 minutes of inactivity, user is disconnected; after 6 hours of inactivity while disconnected, user is logged out
	E-School	60 minutes

- The Information Technology Department provides the employee with a specific password to log in into his/her workstation. The employee is required to change the generated password to a unique password known only to the employee. Each employee has a unique user ID and password to access the network, email, and various applications. Activities conducted within the network and NVision are traced to each specific user. User IDs and passwords for the Active Directory are automatically linked to their access to the Google domain and their respective account.

- Passwords for the Active Directory and NVision are encrypted and consist of letters, numbers and special characters and must be at least seven (7) characters long. Establishing a minimum amount of characters and allowing different types of characters per password reduces the chance of access from someone who is not the user.

- The Information Technology Department has developed controls whereby if a user enters the wrong password his/her logon ID will be automatically locked out as follows:

Server/Application	Unsuccessful Attempts
VDI Server/Active Directory	Five (5)
NVision	Three (3)
E-School	Three (3)

Users that have forgotten their password are required to notify the Information Technology Department. The Administrator of Technology and District Senior Systems Engineer are the only users with sufficient privileges to reset the password and unlock a user's logon ID.

- The Information Technology has developed controls whereby users are required to change their passwords as follows:

Server/Application	Password Change
VDI Server/Active Directory	Annually
NVision	Every Ninety (90) days
E-School	Annually

Narratives of Information Technology Data Security Procedures
Exhibit 6

Active Directory

- The Information Technology Department has segregated the District's Active Directory by groups in separate virtual servers within the District's Virtual Desktop Infrastructure (VDI) server as follows:

  - Administrators/Clerical
  - Teachers (By Building)
  - Students (By Graduation Year)

  Access to shared and/or confidential information is restricted to the respective Administrators and employees in order to prevent unauthorized users to view, alter, delete, or steal this information. The Information Technology Department has access to all active directory folders.

- The Information Technology Department reimages laptops borrowed by employees and/or students to default settings on an annual basis or when their workstations need to be repaired and repurposed.

- The Information Technology Department has developed controls whereby users do not have access to save data on their workstations. Currently, users save their data directly to the servers as they are connected to their virtual desktop.

NVision

- The Assistant Superintendent for Business periodically monitors the following audit trail reports available in NVision:

  - Manual checks
  - Vendor name changes
  - Vendor payments above $10,000

- The Assistant Superintendent for Business reviews the payroll changes report for each payroll period and signs off upon approval.

Google Drive / File Stream

The Information Technology has developed a District wide Google domain with the same structure as implemented for the District's Active Directory and user accounts are automatically linked between the two (2) systems.

Narratives of Information Technology Software Security Procedures
Exhibit 7

The District utilizes the following software:

Operating Systems:

Mac OS 10 or later
Windows 7.0 or greater
Apple iOS 7 or greater
Chrome OS

Office Management/Administrative Software

MS Office 365 Professional (Productivity suite)
NVision

Instructional & Curriculum Software/Research Database

Active Inspire
ADM-Assessment Data Manager
Adobe Air
Adobe CS4
Adobe Flashplayer
Adobe Premiere Elements 11
Adobe Reader
Adobe Shockwave
All Windows Updates
App Inventor 2
Audacity 2015
Auto CAD 2012- English 2015
Autodesk 123 Design
Autodesk Design Review 2015
Autodesk Fusion 360 2015
Autodesk Inventor HSM
Autodesk Inventor Professional 2015
Autodesk Vault 2016
Basic Stamp Editor
BlueJ
C++ Builder5
Celestia
Convert
Corel WinDVD
CURA 3D
Dia
DWG True View 2016
Eclipse
EclipseFRC 2016
Finale

GarageBand
GeoGebraPrim and GeoGebra
Gimp2
Google Chrome
Google Earth
Google SketchUp 8
Inkscape
Inspiration
Internet Explorer 11
Inventor Fusion 2012
Java
Java Developer Kit (JDK)
Jcreator LE
Kidspiration
Lame for Audacity
Learn About Machines
Learn About Weather
Logger Pro 3.8.4
MD Solids 3.5
Microsoft Office Access 2013
Microsoft Office Excel 2013
Microsoft Office InfoPath 2013
Microsoft Office OneNote 2013
Microsoft Office Outlook 2013
Microsoft Office PowerPoint 2013
Microsoft Office Publisher 2013
Microsoft Office Word 2013
Microsoft Visual Studio Express
MinecraftEDU
Mozilla FireFox
National Instruments MultiSIM 12

NetBeans
Notepad++
NWEA Browser
Packet Tracer
Parallax Basic Stamp Editor
PDF Architect
PDF Creator
Pearson Browser
Photo Story 3
Premiere Elements ver 11.0
Psych Corp Center - II
Python
QuickTime
ReadPlease 2003
Revit Architecture 2017
Robix Rascal
Robix Usbor Nexus
Robix Usbor Nexway
ROBO Pro
Roxio Creator Business
SBS Scoring Pro
Scratch
SMART Music
SMART Notebook
Stykz
SweetHome 3D
The Graph Club 2.0
TI Connect
TI Smart View
TOWL4
Type To Learn 3

Type To Learn Jr.
Virtual Tensile Tester
Visio
Vision
VLC Media Player
VMware Player
Vowels Long And Short
West Point Bridge Designer 2015

Win Cupl
Windows Live Movie Maker
Windows Live Photo Gallery
Windows Movie Maker 2.6
Windows-7
Wizard Test Maker ver. 13.0.08
LANGUAGE SOFTWARE
EduGame Interactive
Classroom System ver 9.0
Installed Languages (for Edugame / Wizard Test Maker)
French 1-2-3
German
Italian 1
Spanish 1
Spanish is Fun
Japanese characters installed and available for MS Word

Narratives of Information Technology Software Security Procedures
Exhibit 7

- 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 Information Technology Department deploys the software and/or updates onto the server and grants access to specific employee types and students. Based on the job position, the users or students access the software through their virtual desktop images.

- The Information Technology Department maintains backups of the purchased software by securing the master copies and the user instructions.

Narratives of Information Technology Network Security Procedures
Exhibit 8

VDI Server

The Information Technology Department has implemented a virtual desktop infrastructure (VDI) in respect to the District's server, which gives users the ability to access their desktops from any workstation as long as they have Internet access. The Information Technology Department has classified the VDI desktop images into three (3) groups for Administrators, Teachers, and Students and has developed controls whereby users only access the District VDI through a secure and encrypted SSL connection.

Network Security Software

The Information Technology Department utilizes the following network security software:

Network Security Software	**Purpose**
GoGuardian	To monitor web activity for Chromebooks
Microsoft System Center - Endpoint	Manages anti-malware policies and Windows Firewall security
NextGeneration SonicWALL	Firewall, anti-virus, content filter to prevent intruders from accessing the District's network
Exchange Online Protection	Spam filter to protect email messages are automatically against spam and malware.

- The Information Technology Department monitors the network security software alerts and reviews the exceptions 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 maintains open network ports on the servers that are encrypted through SSL DigitCert for specific applications. 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 grants VPN access for limited periods to vendors such as NVision, E-School, and Third-Party Administrators to conduct their support services. These vendors are given temporary credentials that are revoked after the need for them has elapsed. The Information Technology maintains a log of their VPN access.

- The Information Technology Department utilizes wireless access District wide. Wireless access points at the building level are protected via password to secure 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 or students. The guest wireless network is subject to the District's web-filtering provisions.

Narratives of Information Technology Network Security Procedures
Exhibit 8

- The Information Technology Department conducts semi-annual penetration tests to identify any vulnerability within the District's network. The most recent penetration test was conducted in January 2018.

Network Permissions

The Information Technology Department has assigned access to the District's network as follows:

- Domain Administration - Full access to all server software with the exception of financial application NVision:
  - Assistant Superintendent for Student Services, Technology & Assessment
  - Administrator of Technology
  - Third Party Administrator No.1
    - District Senior Systems Engineer
    - Remote Support Lead
    - Lead Wireless Engineer and Technician
    - Account Manager and Senior Engineer
    - Senior Virtualization Engineer
    - Data Infrastructure Engineer
    - Senior Data Infrastructure Engineer Lead
    - Senior Firewall Engineer
    - Senior Remote Support Technician
  - Third Party Administrator No.2
    - Lead Technician
- Local PC Administration access and permissions to join domain only:
  - Third Party Administrator No.2
    - Level 1 Technicians (5)

Narratives of Information Technology Physical Security Procedures
Exhibit 9

Server Rooms/Main Distribution Frames

- The Information Technology Department maintains twenty (20) physical servers at the Administration building and High School and approximately fifty (50) virtual servers throughout the District. A network schematic is included within the District's Technology Plan.

- The Information Technology Department escorts, supervises and maintains a log of the applicable individuals accessing the District server rooms.

- The two (2) server rooms have air conditioning units installed to maintain a constant temperature and portable fire extinguishers in the event of fire.

- The Information Technology Department has plugged all equipment in the server rooms 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. The server room at the Administrative building is supported by natural gas generator to provide electrical power in the event of blackout. The two (2) server rooms have a power switch to disconnect the circuit between the servers and the power supply in the event of emergency.

Portable Equipment

- The District allows certain Administrators, Teachers, and students to take laptops off school property in order to perform their respective job duties. These individuals are required to sign an "Teacher-Admin Request to Take Computer Equipment" agreement form indicating their acknowledgement 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 are authorized to take laptops off school property.

- The Information Technology Department performs repair services on information technology equipment.

Narratives of Service Continuity Procedures
Exhibit 10

Active Directory/Emails

- The Information Technology Department utilizes Veam software to perform nightly backup snapshots of the District's active directory and emails. The snapshots are incrementally saved onto the District's full backup stored in a separate server located at the Administrative building. The Information Technology Department also stores monthly full backups into tapes that are safeguarded in a fire safe at the Middle School Warehouse. The District maintains monthly backup tapes for seven (7) years.

The District does not store backups of the District's Active Directory or emails outside of District premises.

- The Information Technology Department performs restoration procedures on an as needed basis. During the restoration procedures. the Information Technology Department validates the data, evaluates the District's disaster recovery plan, and ensures that the data are successfully restored onto the network.

The Information Technology Department has not conducted a full-back restoration of the District's servers to verify that the stored data can be retrieved in case of a disaster.

NVision

- The Information Technology Department performs nightly backups of the NVision database and forwards through a secure FTP channel to Suffolk BOCES. Suffolk BOCES also maintains offsite backup in Holbrook NY and in West Seneca NY.

E-School

- The student management system, E-School, is a web-based application and the student data is backed up by the company within its own servers.

Disaster Recovery Plan

The Disaster Recovery Plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the server rooms at the Administration Building and High School.

This disaster recovery plan has the following primary objectives:

- Bring individuals to safety.
- Prevent the loss of the District's resources such as hardware, data and physical information technology assets.
- Minimize downtime related to the disaster.
- Provide an orderly course of action for restoring critical computing capability.

The plan's approach from disaster to recovery involves the following steps:

Narratives of Service Continuity Procedures
Exhibit 10

1. Disaster identification and declaration
2. DRP activation
3. Communicating the disaster
4. Assessment of current and prevention of further damage
5. Establish IT operations
6. Repair and rebuilding of primary facility