Wantagh Union Free School District
Report on the Internal Controls of the Information Systems Cycle
June 2020

Table of Contents

I. Scope of Engagement

The Board of Education of the Wantagh 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 Information Systems Cycle. As part of this engagement, we performed extensive analysis and validation tests within the District's Information Systems Cycle.

The objective of our analysis was to determine whether the internal controls pertaining to information systems 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 information systems 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 Information Systems Cycle after interviews and discussions with key employees

- Identified key controls within each functional area of the Information Systems Cycle and performed audit tests of those controls

- Performed a walk-through of various information systems locations

- Made observations and recommendations pertaining to the internal controls of the Information Systems Cycle based upon observations and testing that was performed

Interviews and inquiries were conducted with the following District employees:

Title	Department
Director of Technology	Information Technology
Assistant Superintendent for Business	Business Office
Assistant Business Manager	Business Office

II. General Controls and Governance

The Wantagh Union Free District has an Information Technology ("IT") Department comprised of six (6) employees, five (5) of which are on-site consultants from Nassau BOCES and Core BTS.

The District's Board of Education adopted several policies pertaining to the acceptable use of the District's computer system as it relates to both staff and students. The District has the following policies in place that address topics such as remote access, internet security, privacy rights, and potential disciplinary action:

- Policy #4526, *Computer Use In Instruction: Network Access and Acceptable Use*
- Policy #4526.1, *Internet Safety*
- Policy #8630, *Computer Resources and Data Management*

Observation and Recommendation #1

III. Network Security

User Access

The Human Resources Department notifies the IT Department when there is a change in employee status ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ The IT Department is responsible for granting and removing access to the District's email and network.

We reviewed Board of Education resolutions for ten (10) employees who were hired or terminated during the 2019-2020 school year to determine the following:

- There is documentation on file showing the activation or inactivation of the user's network/ email user account
- Employees are included on an active listing from the District's financial accounting and terminated employees are no longer included on the active listing

Observation

We noted that the ten (10) employees selected for testing had documentation on file showing the activation or inactivation of the user's network/email user account and employees are included on an active listing from the District's financial accounting and terminated employees are no longer included on the active listing.

No recommendation at this time.

Observation and Recommendation #2

██

■ ██
████████████████████████████████

We also reviewed an Active Directory listing, which includes ████████████████████ user accounts that have access to the District's network, to ensure that only active employees or consultants are included on the listing.

Observation and Recommendation #3

██

➢ ██

Remote Access

██

Observation and Recommendation #4

██

➢ ██

Observation and Recommendation #5

██

> ███
> ███████████████████████████████

IV. <u>Financial Application Security</u>

The Assistant Business Manager in the Business Office is responsible for granting and removing access to the District's financial accounting system, nVision. The Assistant Business Manager is aware of new or terminated employees through review of the Board of Education agendas. Users are assigned roles that are required for their job duties. Roles can be customized to limit permissions.

We obtained the Role Membership Report from the nVision financial application as of November 12, 2019, consisting of ███████ active user accounts. We compared the Role Membership Report to the District's active employee listing to confirm that all only current employees have active user accounts.

<u>Observation and Recommendation #6</u>

███
███
███

> ███
> *We also recommend that the District develop a standard form to notify the Assistant Business Manager when employees are hired or terminated in order for access to be granted or restricted. Requests for changes to permissions should also be formally requested and approved to ensure proper authorization.*

<u>Observation and Recommendation #7</u>

We noted ten (10) users whose permissions appear to conflict with or not be necessary for their position and job responsibilities.

> *We recommend that the District review the permissions assigned to the users identified and determine if adjustments are needed.* █████████████████████████

V. <u>Inventory</u>

The IT Department utilizes an Access Database to maintain and track fixed IT assets. All IT assets are entered into the database, regardless of the cost. The IT Department employees are responsible for tagging and tracking the location of assets. The make, model, serial number, asset tag and location of each asset are recorded in the database. The IT Department also keeps separate inventory lists for Chromebooks. The Chromebook listing includes the asset tag number, serial number, MAC address, and user.

It should be noted that inventory records were not provided by the District so an inventory observation could not be completed.

VI. Disaster Recovery

A school district's network, servers, software, and data are essential to the financial and instructional day to day operations. Therefore, it is in a school district's best interest to prepare a disaster recovery plan to document backup procedures as well as procedures for data recovery and restoration of the District's network and servers in case of an emergency or disaster.
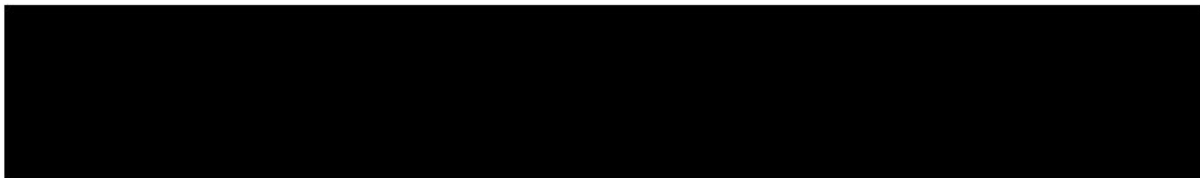
███
███
███
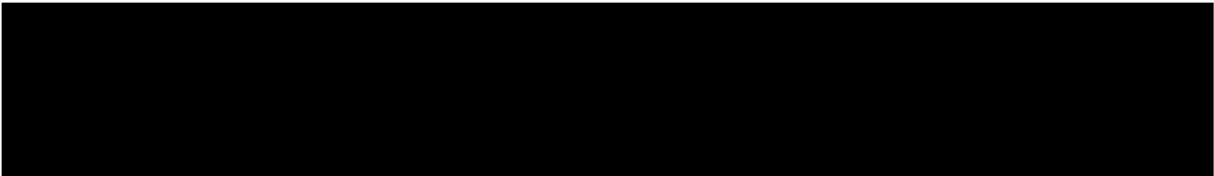
Observation

███
███
███
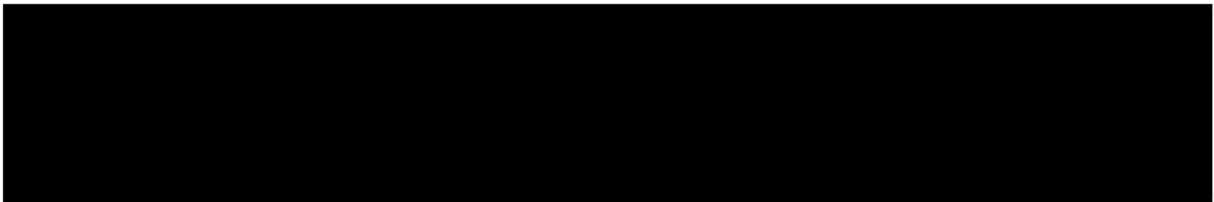
> ➤ *No recommendation at this time.*

VII. Facilities

███
███
███

It should be noted that a walk-through of server rooms was not completed due to COVID-19 school closures.

VIII. Risk Rating and Audit Opinion

Inherent Risk: ████████████
Control Risk: ████████████
Audit Opinion: ████████████

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

Auditors Spoke with:

Director of Technology – Penny Curry
Assistant Superintendent for Business – Anthony Cedrone
Assistant Business Manager – Maureen Barclay

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

I.	General Controls and Governance
II.	Network Security
III.	Financial Application Security
IV.	Inventory
V.	Disaster Recovery
VI.	Facilities

Blue = Internal Control

I. General Controls and Governance

- The Wantagh Union Free District has an Information Technology ("IT") Department comprised of six (6) employees, five (5) of which are on-site consultants from Nassau BOCES and Core BTS.
- The Director of Technology maintains a list of employees with their general job duties.
- Policy #8630 *Computer Resources and Data Management*, approved by the Board of Education in August 2017, directs the Superintendent and Director of Technology to oversee computer resources and establish regulations to govern the use and security of those resources.
- In addition to the above noted policy, the following, with Board of Education adoption or amendment dates, are also in place regarding Information Technology:
  - Policy #4526 *Computer Use in Instruction: Network and Acceptable Use*, July 2019
  - Policy #4526.1 *Internet Safety*, July 2019
  - Policy #8635 *Information Security Breach and Notification*, August 2017
- The District also has a Technology Committee that is comprised of administrators and employees representing each school building, grade level and department. Meetings serve as a means to discuss any issues or new plans with the Director of Technology.
- The Technology Committee is responsible for updating the District's Technology Plan.
- IT Department employees and consultants will attend training courses throughout the year that correspond to their job duties.
- The Director of Technology works with the Assistant Superintendent to develop the annual IT budget.
- The IT budget is impacted by the District's five year technology plan and any fees related to renewals or purchases of new software applications.

II. Network Security

- The IT Department receives notification of new employees from the Human Resources Department.
- The Human Resources Department will update ██████████████████████ for the IT department for any new hires and terminations. ████████████████ is used by IT to track when access is granted and disabled.
- The new employee's position indicates the different application access and permissions that an employee will need. For example, access to the student data management software would be given to teachers, but not to buildings and grounds employees.
- The IT Department is responsible for granting and removing access to the District's network and student data management program, E-School.
- ██
- ██
- ██
- ██
- ██
- ██
- E-School has generic permissions for teachers and staff. These permissions are granted based on the employee's position and any changes are processed by the IT Department.
- ██
- ██
- ██
- ██
- ██
- Go Guardian is installed on Chromebooks issued to students. Go Guardian is a web filter that also sends alerts to the Director of IT and building principal if the student attempts to access malicious or inappropriate material.
- ██
- ██
- ██ Employees can access the wireless network by logging in on their device with their District network user name and password.
- Students cannot connect personal devices to the District's wireless network.

III. Financial Application Security

- The Assistant Business Manager in the Business Office is responsible for granting and removing access to the District's financial accounting system, nVision.
- The Assistant Business Manager is aware of new or terminated employees through discussions with the Payroll Department employees or review of Board agendas.
- Users are assigned roles that are required for their job duties. Roles can be customized to limit permissions.

▪ ██

▪ ██
▪ ██

▪ ██
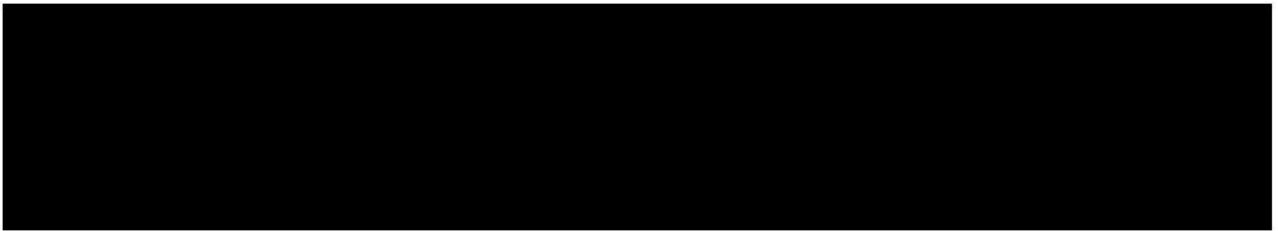
IV. Inventory

▪ Policy #6645 *Inventory and Fixed Assets Accounting,* last updated in April 2017, states that the Board of Education will establish a dollar threshold for considering which assets are to be depreciated. The current threshold is $5,000.

▪ The Business Office is responsible for tracking assets that meet the capitalization threshold. The Business Office staff will record the asset, make, model, serial number and asset tag.

▪ The IT Department maintains an inventory listing of all assets regardless of the cost.

▪ The IT Department logs assets into an Access Database. The Access Database is used to track the make, model, serial number, asset tag and location.

▪ The IT Department is in the process of converting the information in the Access Database to a new system. Until the new system is fully implemented, the IT Department will have information in two (2) separate databases.

▪ The IT Department also keeps separate inventory lists for Chromebooks. The Chromebook listing includes the asset tag number, serial number, MAC address, and user.

▪ Shipments are received by the IT Department employees. If the shipment is for a specific school, the tech that is in charge of that building will open the shipment.

▪ ██

▪ ████████████████████████

▪ Administrators, teachers and students in grades six (6) through twelve (12) are issued Chromebooks that can be taken off of District property. All users sign a form to acknowledge that they've received a device from the District.

▪ Students at the elementary level use Chromebooks, but they cannot be taken off District property. They are maintained in a charging cart when not in use.

▪ The IT Department maintains a list of software currently in use by the District. The list is updated as new software is purchased and old software is removed.

▪ Requests for new student related software are sent to the Director of Technology. The Director of Technology will review system requirements and user agreements prior to approving the software purchase.

▪ The teachers requesting the software will typically download a trial version to use with the students before requesting the purchase.

▪ Only the IT Department can install or update software on District devices. The ability to install software is disabled for users.

▪ The Director of Technology determines which assets require disposal. Factors considered include the asset's use, life span, broken parts or ability to install required upgrades.

▪ The Director of Technology sends a list of assets for disposal to the Assistant Superintendent for Business to include on the Board agenda.

▪ All assets disposals are documented and presented to the Board of Education for approval before being removed from inventory.

V. Disaster Recovery

- A school district's network, servers, software, and data are essential to the financial and instructional day to day operations. Therefore, it is in a school district's best interest to prepare a disaster recovery plan to document backup procedures as well as procedures for data recovery and restoration of the District's network and servers in case of an emergency or disaster.
- The Disaster Recovery Plan should identify the data backup plan for critical data, the location of backup servers, and the process to access critical data and continue operations in the event of a disaster.
-

-

-

-
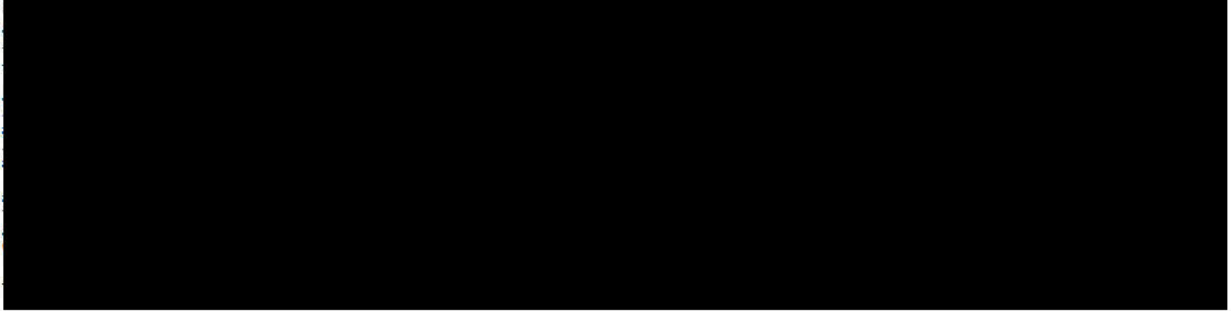
VI. Facilities

-

-
-

-
-

-

-

-

-
- Technology equipment is protected by smoke detectors and fire extinguishers located throughout the District.