



**Review of
Information Technology Environment
and
Access Permissions**

APRIL 2017

April 2017

The Board of Education
The Plainview-Old Bethpage Central School District
106 Washington Avenue
Plainview, NY 11803

Board of Education:

We have been retained to function as the internal auditor for the Plainview Old-Bethpage Central School District (hereinafter, "the District"). Our responsibility is to assess the internal control system in place for the accounting function within the District, and to make recommendations to improve upon certain control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District's Board, management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND

We had assessed certain aspects of information technology controls and issued reports to the Board in June 2008 and March 2009. We also assessed the adequacy of internal controls over the protection of personal, private, and sensitive information (PPSI) and issued a report of our review and recommendations June 2013. As this area was tested several years ago, and there have been significant changes in technology, the Audit Committee requested that internal audit reassess the internal controls within the information technology environment. The results of our review are documented in Section I of this report.

In addition, we assessed the adequacy of access permissions to key District applications including WinCap (financial management system), Infinite Campus (student management system), and IEP Direct (special education management system). The results of our review are documented in Section II of this report.

SECTION I. INFORMATION TECHNOLOGY ENVIRONMENT

The Information Technology (IT) department has prepared a comprehensive Technology Plan that details the District's current computing environment, and the recommendations needed for handling future growth. To achieve the objectives of increased use of technology, the District has outlined implementations using the Smart School Bonds Act funds. The District has created a Smart School committee to discuss current and future technology needs in order to support academic requirements, and is comprised of stakeholders from all segments of the school community including parents, teachers, students and other community members who are leaders of the non-public school in the community. The committee recently agreed that the primary focus of the plan should incorporate installing a district-wide high-speed wireless connectivity consistent with the District's Instructional Technology Plan.

The IT functions in the District are performed under the direct supervision of the Director of Technology. The District's information technology services are managed by Nassau BOCES, which includes providing daily systems support, network access support, as well

as a backing up and restoring data. To perform the review, we utilized the Information Technology (IT) Systems Self-Assessment Questionnaire from the Information Technology Guidance produced by the New York State Comptroller's Office, as well as an internally created IT Questionnaire. The questionnaires were completed by staff from Nassau BOCES. Our objective was to assess the District's internal controls to determine if computer equipment, software, and data are adequately safeguarded. To perform our review of the information technology environment, we discussed the roles and responsibilities of District staff and Nassau BOCES staff, and assessed the controls that are in place that relate to information technology, focusing on policies, access controls, and continuity of business operations. The District has made significant progress in upgrading the technology infrastructure and increasing accessing security controls. We noted areas where internal controls over the IT environment can be further strengthened. The recommendations are indicated below.

A. INFORMATION TECHNOLOGY POLICIES

The Board is responsible for adopting formal policies focused on protecting data and hardware from loss or misuse due to errors, malicious intent or accidents (e.g., disasters). Therefore, it is essential that the Board establish policies that include password management; wireless technology; remote access; use of mobile devices; data backups; sanitation and disposal of electronic media; breach notification; user accounts; access rights; and the protection of personal, private and sensitive information (PPSI). The District's website has several key IT policies including a District Computer Network/Internet Safety and Use Policy and Guidelines for students and teachers. Technology policies are reviewed annually and amended as appropriate to reflect changes in technology or the District's computing environment. While the Board has most of these policies in place, we noted the following.

Issue #1: While the District has internal procedures for the disposal of obsolete IT equipment, and has a policy for the disposal of District property, the policy does not contain procedures for the sanitization and disposal of such equipment.

Risk: Increased risk of personal and confidential data being recovered and inappropriately used or disclosed by unauthorized individuals.

Level: Moderate-High

Recommendation: We recommend that the Board revise policy #5250: Sale and Disposal of School District Property, to require sanitization of hard drives or other electronic media before disposing.

District Response:

The District currently has a practice of sanitizing hard drives and electronic media prior to disposing. Management agrees this should be included in policy and will suggest a revision to the Policy Committee.

Issue #2: The Board has not adopted a wireless security policy. Such a policy includes practices to safeguard data when collecting, storing, or transmitting confidential information.

Risk: Increased risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use.

Level: Moderate-High

Recommendation: We recommend that the Board adopt a wireless security policy that specifies the conditions that wireless infrastructure devices must satisfy to connect to the entity's network. The policy should also indicate who is covered by the policy (e.g., all employees, contractors, consultants, temporary, and other workers) and describe the consequences of violating the policy.

District Response:

Management agrees this should be included in policy and will suggest a revision to the Policy Committee.

B. WIRELESS ACCESS

Wireless networks (Wi-Fi) are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access, and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air. These traveling signals can, potentially, be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, the security problems of a wireless segment can affect an entire network. A wireless environment, therefore, requires certain additional security precautions.

Issue #3: The District's expansion of the wireless access through Wi-Fi does not include requiring a password, and does not require confirmation of the identity of the user. By not authenticating users, the District cannot control what the user is accessing.

Risk: Increased risk that inappropriate access can occur and cannot be readily managed.

Level: Moderate-High

Recommendation: We recommend that the District require a password to access Wi-Fi, and access should require users to be authenticated.

District Response:

Management acknowledges this recommendation. The district will implement WPA2 personal authentication. Credentials will be supplied to visitors for access to the guest/BYOD network.

C. REMOTE ACCESS

The District permits certain staff and vendors to remotely access the District's network and select applications using a secure Virtual Private Network (VPN). The benefit of using a secure VPN is it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.

Issue #4: We noted that access via VPN was provided to a vendor to access the District's student information database, Infinite Campus, using a generic user name, rather than a specific user name. As such, the District cannot determine who is actually accessing the system and if that access is appropriate.

Risk: Increased risk of unauthorized access.

Level: Moderate-High

Recommendation: We recommend that the District require a specific user name to be assigned to the vendor when accessing the District's network via VPN. In addition, the Director of Technology should be periodically reviewing the access logs to ensure the access was appropriate.

District Response:

The District will work with the sole vendor that has VPN access to the District's network in order to identify two vendor employees that will have VPN access. Management notes that the vendor has access to specific IP addresses within the buildings that are assigned to energy management systems.

D. DATA BACKUP

The District is utilizing Nassau BOCES to replicate data off-site to be used as a backup in the event the District's systems are compromised.

Issue #5: We noted that current version of the District's financial software application WinCap is several years old and cannot be virtualized. As such, data cannot be automatically backed-up and restored remotely.

Risk: Increased risk of loss of data.

Level: Moderate-High

Recommendation: We recommend that the District implement the latest version of WinCap so that Nassau BOCES can automatically back-up the data.

District Response:

District management thanks the auditor for bring this issue to our attention. The District will develop a plan in order to update WinCap to its current version with the least disruption to District operations. WinCap will then be virtualized. District Administration notes that WinCap data cannot be hosted by Nassau BOCES, but that Nassau BOCES employees can assist in updating the WinCap software.

E. PHYSICAL SECURITY ACCESS

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss, or impairment. Such controls can also include environmental controls such as smoke detectors, fire alarms and extinguishers, protection from water damage, and uninterruptible power supplies.

Auditor's Comment: While the physical controls adequately restrict access to the District's Network Operating Center (NOC), the District can strengthen controls by installing a camera inside the NOC to monitor access.

District Response:

A camera will be added to the NOC as part of a security upgrade project that will commence in April 2017.

F. IT EQUIPMENT INVENTORY

Maintaining detailed, up-to-date inventory records for all computer hardware is essential so that the current technology infrastructure is accurately represented, and so that future technology needs can be determined. The information maintained for each piece of computer equipment should include a description of the item including the make, model, and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date. The District is utilizing the application School Dude to indicate the asset tag number, disposal information, and movement of equipment. We noted that Nassau BOCES recently performed an inventory of the items listed in School Dude.

Auditor's Comment: The District can strengthen the internal controls over tracking computer hardware by implementing an automated inventory asset management application. Such a system can reduce the risk of errors in inventory records resulting from manual entry, can reduce the time needed to perform periodic inventories, and can increase accuracy of inventory records.

District Response:

The district is already tracking its IT equipment inventory in SchoolDude. The district will look to expand on the system's functionality. The district will look to take advantage of barcode-based data entry, user tracking accountability and mobile inventory scanning.

SECTION II. REVIEW OF ACCESS PERMISSIONS

As part of this review, we also examined the access permissions assigned to key applications: WinCap (financial management system), Infinite Campus (student management system), and IEP Direct (special education management system) to determine whether access rights were appropriately assigned. Access permission controls are intended to provide reasonable assurance that computer resources are protected from unauthorized use and modifications. To perform this evaluation, we gained an understanding of how access is granted and then verified that the access permissions within each of the three applications is properly restricted, that proper segregation of

duties exists, and that access is limited based on the user's job descriptions and responsibilities.

A. WinCap

The WinCap application is comprised of several sub-system modules for performing various financial and human resources functions. The District utilizes the following modules:

- Financial - purchasing, accounts payables and cash disbursements, budget maintenance and development, revenue accounting, general ledger, cash receipts, billing and accounts receivable, and payroll.
- Human Resources - personnel management (employee attendance, appointment earnings, fingerprint information, health benefit information), professional management (tenure and certification information)

WinCap has the ability to produce a log indicating when, where, and who uses the computer system. It can also generate a log of all changes made to the information included in the vendor master files. Because virtually all District accounting records and reports are computer generated, it is important that District officials review audit logs periodically. Without such a review, the District does not have adequate assurance that changes to its financial information are appropriate and authorized. We noted that the Assistant Business Administrator reviews payroll comparison reports as well as payroll edit logs periodically throughout the year.

Access to WinCap including designating user access rights as well as access to the specific applications within WinCap, is performed by the Assistant to the Superintendent for Health, Safety & Transportation. The functions are correlated to specific accesses that can be performed within that module, and access can vary from view only to all access. Permissions to WinCap and the specific applications, including any changes, are documented on forms that are reviewed and approved by the Assistant Superintendent for Business Operations or the Assistant Business Administrator, and then performed by the Assistant to the Superintendent. WinCap automatically requires users to change their password every 90 days.

We selected 16 access forms prepared in the current school year and noted the forms were appropriately approved and that access within WinCap was as stated on the form. We then reviewed the User Security Profile Report dated October 11, 2016 and evaluated the appropriateness of the access permissions assigned for those who had access to payroll, human resources, accounts payable, and system administrator functions. Based on the access capabilities listed, we assessed if the permissions granted are those functions needed to be performed within the selected employees' job duties, and that each employee is restricted from performing multiple aspects of a financial transaction that could compromise proper segregation of duties.

Based on our review of the access permissions assigned within WinCap, access appears to be appropriately assigned, and the accesses granted are based on job functionality.

Issue #6: We noted that if users forget their password, the user can call the Assistant to the Superintendent to have the password reset; however, there is no written documentation to support the request or the action performed.

Risk: Increased risk of unauthorized access.

Level: Moderate-High

Recommendation: We recommend that the District require any requests for a password reset to be done through the District's IT help desk system to document the request and verify the authenticity of the user requesting the password change.

District Response:

Management will put a process in place in which password reset requests are sent to the help desk via email where the emails are saved via the email archiver.

B. INFINITE CAMPUS

Infinite Campus is the District's student management information system, and is utilized for creating student schedules, tracking student attendance and enrollment, and recording student grades. This system also links with IEP Direct (special education). Users are assigned access to specific groups that allow the user to perform specific functions within Infinite Campus (e.g. a group may only have "view" capabilities). The groups are correlated to a set of specific activities that can be performed within the system. Access to each activity can be further restricted by the ability to view or modify data based on need, such as restricting a teacher's access to only current year students.

To review access permissions, we requested the User Rights Report for 15 employees in the District, which included teachers, principals, directors, nurses, and assistant superintendents. Based on our review of the access permissions assigned within Infinite Campus, access appears to be appropriately assigned, and the accesses granted are based on job functionality.

Issue #7: We noted that requests for access are not formally documented to support the request or the action performed. Currently, users request access to Infinite Campus either via a phone call or an email. We also noted that the application does not log when changes are made to a user's access by the system administrator.

Risk: Increased risk of unauthorized access.

Level: Moderate

Recommendation: We recommend that all access requests or changes in access to Infinite Campus be formally documented and approved to ensure the access is appropriate. In addition, we recommend that the District implement the feature within Infinite Campus (Data Change Tracker) to capture who made changes and when. The log should be periodically reviewed by District Management to ensure changes made are appropriate, and to expose any anomalies.

District Response:

Management will put a formal process to document access requests/changes in Infinite Campus similar to that used to request changes in WinCap permissions. Management will research Data Change Tracker and make an informed decision regarding its purchase and implementation. Data Change Tracker is primarily used to track changes in the Infinite Campus database; not to track who has permissions to the various levels of utilities within Infinite Campus.

C. IEP DIRECT

The software application, IEP Direct, enables the District to document and track special education services provided to District students. This system utilizes the database information from Infinite Campus (e.g., student class lists) allowing data to be integrated automatically. Data is also shared between IEP Direct and Infinite Campus through the Schools Interoperability Framework (SIF) compliance feature within IEP Direct.

Actions performed within IEP Direct automatically track the user ID and the date of access. IEP Direct has several reporting features that enable the District to verify the records. The District utilizes Centris Sync to import demographic information directly from Infinite Campus, and as such, these changes can only be made in Infinite Campus. Changes made to the student's IEP are based on the recommendations from the CSE and are reviewed by the staff responsible for the student's IEP before the IEP change is finalized. The IEP cannot be changed except by the systems administrators.

Access to IEP Direct is the responsibility of the Executive Director of Pupil Personnel Services and Special Education. Users are assigned access rights within IEP Direct based on group profiles, which lists the specific accesses that can be performed within each group. Within each group, users are further grouped according to their job function and are restricted to view only /edit of certain records (e.g. a special education teacher only has access to those students assigned to the teacher's class). The Executive Director of Pupil Personnel Services and Special Education can further restrict an individual's access to specific functions within the group based on job responsibility. The District also requires that anyone given access to IEP Direct is required to sign a confidentiality and non-disclosure agreement.

The District utilizes the following access group profiles:

- Central Office Level, Supervisor
- Central office Level, Edit
- Central Office Level, View
- Central Office Level, Data Entry (no users assigned)
- School Building Level, Supervisor
- School Building Level, Data Entry
- School Building Level, View
- School Building Level, Edit
- Student Level Data Entry
- Student Level View
- IEP Provider
- Evaluator/Provider Only

We obtained a list of all users with access rights within IEP Direct as of October 20, 2016. We then obtained a list of group profiles which lists the specific accesses that can be performed within each group. Utilizing the report of all users' access permissions, we analyzed the individuals assigned within each group. Based on the list of users within each group, we assessed if the permissions granted are those functions needed to perform their job duties, and that the employee is restricted from performing actions that could compromise proper segregation of duties (i.e. a teacher being able to change an IEP of a student that is not assigned to them). We also reviewed a sample of 25 users and verified that a confidentiality and non-disclosure form was signed.


Based on our review of the access permissions assigned within IEP Direct, access appears to be appropriately assigned, and the accesses granted are based on job functionality.

We would like to thank the staff at the District for their cooperation and professionalism during our testing.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

A handwritten signature in cursive script that reads "Cerini & Associates LLP".

Cerini & Associates, LLP
Internal Auditors