



Plainview-Old Bethpage Central School District

Review of Personal, Private, and Sensitive Information (PPSI) on Mobile Computing Devices And Computer Equipment Inventory

June 2013

June 2013

The Board of Education
Plainview-Old Bethpage Central School District
Plainview, NY

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 Board, the District's management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND

We have assessed certain aspects of information technology controls and issued reports to the Board in June 2008 and March 2009. We were requested to assess the adequacy of internal controls over the protection of personal, private, and sensitive information (PPSI) by the Audit Committee during the December 2012 meeting. The State Comptroller's office defines PPSI as "any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or citizens of New York in general." Private information could include social security numbers, health records, credit card data, student test results, student psychological analyses, driver's license numbers, security codes, or access codes/passwords that would permit unauthorized access to protected staff or student records.

Technology has shifted from the traditional desktop environment to handheld devices that permit users to perform similar functions without being constricted to one location. Such mobile computing devices (MCDs) include tablets, smartphones, personal digital assistants (PDAs), laptops, and netbooks. While such portability has facilitated employee productivity and allowed for greater and faster communications, these devices can introduce security vulnerabilities that did not formally exist.

SCOPE AND TESTING

The objective of our review was to determine whether the District has adequate policies and procedures to control and protect confidential information on MCDs. To assess this, we performed the following:

- Interviewed key management responsible for implementing District policies and procedures to gain an understanding of the internal controls to protect such information;
- Reviewed the current policies and procedures currently in place and assessed that they adequately address the risks of exposure of PPSI; and
- Selected and reviewed a sample of mobile computing devices to ensure access to the device is restricted.

As the District's use of computer technology continues to increase, it is important that the District has comprehensive and effective internal controls to ensure that computer equipment is properly safeguarded and inventoried. The dissemination of tablets (e.g. iPads and Surfaces) in the District is controlled, tracked, and monitored by the Business Office in conjunction with the Special Education/Pupil Personnel Services Office. The inventory of all other computer-related equipment (i.e. desktop computers, servers, netbooks, notebooks, printers, document scanners, digital cameras, SmartBoards, printers, etc.) is separately controlled, tracked, and monitored by the Information Technology department. As such, our review focused on assessing the internal controls in place surrounding the inventory processes. Our review involved:

- Assessing controls over safeguarding of computer equipment.
- Assessing the procedures for recording computer equipment in the District's asset management software application, School Dude Asset Inventory (School Dude), including when equipment is transferred or deemed obsolete.
- Comparing the computer equipment inventory information recorded in School Dude Asset Inventory to the actual inventory at the various schools to determine if the District is maintaining accurate records.
- Assessing the procedures for recording and tracking MCDs.

Based on our interviews, observations, and assessments performed, the District has established effective internal controls over the protection of PPSI on MCDs as well as over the physical whereabouts of MCDs and computer equipment. The results of our review are detailed below:

A. Policies & Guidelines

Good governance and accountability require the District's Board to adopt policies and procedures to safeguard PPSI against unauthorized access, misuse, or abuse. The State Comptroller's Office performed a review of PPSI at 12 upstate school districts, and in their report issued December 2012, they cited several policies that would address the various aspects

of securing confidential data and limiting access to it. Such policies include encrypting data on MCDs, ensuring remote access to District resources is performed in a manner consistent with acceptable use guidelines, restricting the use of sensitive information in email communications, limiting and restricting non-District MCDs from gaining access to District resources, and ensuring procedures are in place should a data breach occur. District's should have specific care and use guidelines for all district-owned MCDs that are given to staff/students, and should require staff/students to sign an agreement regarding care and use of district-owned MCDs.

The District has adopted or has drafted several policies as well as procedures that encompass PPSI concerns noted by the Comptroller's Office. These include:

- Employee Personal Identifying Information
- Information Security Breach and Notification
- Technology Security Management
- Student/Staff Use of Personal Mobile Devices (PMD) Building-based Guidelines
- Internet Safety and Use Policy
- Staff/All User Access to the District's Computer Network and Internet
- Computer Network and Internet Safety and Use Guidelines
- Use of District Owned MCDs Procedures and Agreement

The draft policies and procedures have been reviewed by the District's policy committee and are currently being reviewed by the District's attorneys. We commend the District's efforts for their proactive measures to ensure that District data is properly safeguarded.

Recommendation: Once the policies and procedures have been adopted, we recommend that the District issue a memorandum to all staff/students to apprise them of proper safeguarding of PPSI on all devices.

Management's Response:

The District agrees with the recommendation to inform all staff/students of newly adopted policies and procedures related to PPSI on all devices. Once the policies and procedures are adopted, we will be sure to forward to all stakeholders accordingly.

B. Access Security Controls over PPSI

As the District's utilizes and relies heavily on computers and related equipment for processing financial and nonfinancial information, proper protection from unauthorized or inappropriate access is a critical internal control. We examined access security controls as part of our review of the Information Technology environment (report dated March 2009) and noted that access to District computer resources requires documented approvals for granting, changing, and terminating access rights. This includes requiring specific access permissions and password controls to limit access to critical and sensitive data. We confirmed that access to the District's network via MCDs requires the same access permissions and passwords as if using the

District's desktop computer. Furthermore, we confirmed that all district used MCDs require and/or will require a password to gain access to the specific device.

Recommendation: To further strengthen access security controls and to ensure access to PPSI is minimized, we recommend that the District restrict storing sensitive information on MCDs where feasible, ensure all MCDs lock after a period of inactivity and require a password to access the device, and assess the feasibility of implementing full disk encryption or installing encryption software, which would prevent unauthorized access should the MCD become lost or stolen.

Management's Response:

The District agrees with this recommendation to further strengthen the securities on MCDs. Attached is a memo that has already been sent to all administrators to address these concerns.

C. PPSI Data Classification and Computer Equipment Inventory

As indicated in the State Comptroller's report on PPSI, a best practice is to have all information, whether in printed or electronic form, be classified by assigning a level of risk to various types of information. The risk level assigned should be based on the criticality of the information and the need for appropriate security protocols. Once classified, the data should be labeled in a consistent manner to ensure data confidentiality, integrity, and availability. This is especially important if there is a data breach due to unauthorized system access or theft of equipment. Therefore, it is essential that inventory of all computer equipment, and in particular mobile computing devices, be documented and an inventory review be conducted to ensure all equipment is accounted for, and that management can determine the appropriate action to take. We noted that the District has created a district-wide data classification scheme, and performs regular inventories of computer equipment (i.e. laptops and netbooks) as well as mobile computing devices (i.e. tablets).

The Business Office maintains inventory of tablets provided to Board members and District administrators, and the Special Education Department maintains inventory of tablets to special education teachers including sets provided for the special education classrooms. To assess the adequacy of inventory controls of tablets issued to various administrators, teachers, and Board members, we verified the whereabouts of 15 devices and confirmed that the inventory records were accurate.

To assess the adequacy of the whereabouts of computer equipment (desktops, document scanners, laptops, and netbooks), we selected sixty (60) items from the District's inventory database to verify the accuracy of the inventory information maintained at the various school buildings. We noted several instances where the District's inventory records in School Dude did not contain the asset tag number but rather the product's serial number, making it more difficult to confirm the accuracy of the inventory records. We were however, able to confirm that the computer equipment

was at the stated location for 58 of the 60 items selected. Of the two items that we could not locate, one item was recently disposed and the other item was temporarily relocated for the summer, however the database was not updated to reflect this. In addition, we selected twenty five (25) items found at the various school buildings to verify the accuracy of information recorded in School Dude. Since our test utilized the asset tag number and the database is still being updated, this test could not be readily performed.

Recommendation: We were informed that the IT Department is in the process of revising the inventory record keeping procedures, which includes tagging all computer equipment, and updating the computer equipment inventory records in the School Dude database to indicate the asset tag number, disposal information, and movement of equipment. We commend the efforts of the IT Department to ensure that the computer equipment inventory records are accurate and recommend once the records in the database are updated, the District perform an inventory check to verify the accuracy of the inventory information.

Management's Response:

The District will perform an inventory check to verify the accuracy of the IT department information. Furthermore, we will explore the cost benefit of a unified inventory data base to help improve accountability in tracking of all District fixed assets.

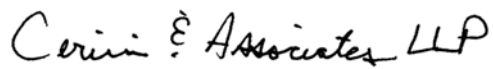
Auditor's Comment: The District maintains inventory of all other capital assets other than computer equipment in a spreadsheet. Every year, the District has CBIZ perform an inventory analysis that provides the District with a list of the current inventory. While confirmation of the inventory is being performed, any changes to the inventory spreadsheet need to be performed manually. The District may want to consider obtaining an inventory database management system for all items that are required to be inventoried per the District's threshold, as well as all computer equipment. The database can then be updated automatically after the inventory is performed by CBIZ. In addition, a unified inventory database can improve accountability as the system can track all inventory transactions including requests, receipt of goods, internal transfers, returns to suppliers, depreciation, and disposals, which will allow the District to better forecast and budget for future needs.

We would like to thank the staff at the District for its 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



Plainview-Old Bethpage Central School District

106 Washington Avenue, Plainview, New York 11803

Office of Human Resources

Timothy T. Eagen, Ed.D
Assistant Superintendent for Human Resources

MEMO

**TO: Board of Education
All Administrators**

FROM: Dr. Timothy T. Eagen

DATE: August 5, 2013

RE: Personal, Private, and Sensitive Information (PPSI) and Passwords

This past summer we reviewed several policies and procedures around personal, private, and sensitive information (PPSI), and we are in the process of making updates. In particular, we have been assessing the adequacy of internal controls over the protection of PPSI (i.e. SSNs, security codes, health records, IEPs, etc...). As we all know, technology has significantly shifted from the traditional workplace desktop to district issued phones and mobile devices (i.e. iPad, Surface, Netbook). While these devices have greatly increased our productive and improved communication, these devices have introduced security vulnerabilities that did not previously exist.

In order to address this concern, please ensure that password protection is enabled on any district issued device. On an iPad, this feature can be enabled by going into... Settings – General – Passcode Lock, and setting it to the “on” position. You will then be prompted to enter your passcode. Please contact either Dr. Lodico or me if you should need any technical assistance.

Thank you in advance for your attention to this matter.