

Mount Pleasant Central School District

825 Westlake Drive
Thornwood, NY 10594

Susan Guiney, Ed.D.
Superintendent of Schools

Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Christopher Ellis, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

RE: Corrective Action Plan - 2009M-131

December 2, 2009

Dear Mr. Ellis:

On behalf of the Mount Pleasant Central School District Board of Education and myself, please accept this Corrective Action Plan in response to the findings and recommendations contained in the Report of Examination of the Mount Pleasant Central School District: Internal Controls Over Selected Financial Activities for the period of July 1, 2007 through December 1, 2008.

The Mount Pleasant Central School District is committed to excellence in each and every aspect of its operations and remains grateful to the Comptroller's Office for their recommendations for continuous improvement over financial controls and activities. As your office is aware, since I was appointed Acting and then Superintendent of Mt. Pleasant, many actions already have been taken to address the recommendations of the report. Additionally, other actions are planned that will completely address all recommendations presented to the district.

The Corrective Action Plan which follows indicates the District's responses to the audit recommendations.

Very truly yours,

Susan Guiney

Susan Guiney, Ed.D.
Superintendent of Schools

Cc: New York State Education Department

Purchasing

1. *District officials should amend purchasing procedures to state when RFPs should be used, identify dollar thresholds for obtaining written or verbal quotations, and describe the type of supporting documentation required for these purchases.*

Corrective Action:

Administrative Manual received and distributed to Administrative Council that outlines purchasing procedures including information about RFPs, dollar thresholds, and competitive bidding.

The Superintendent has reviewed policy and procedures with the Business Office staff.

The Superintendent has reviewed policy and procedures with the Superintendent of Buildings and Grounds to ensure that public works contracts under the statutory threshold for competitive bidding are obtained following the Board's procurement policy.

Purchasing procedures distributed to building principals and office staff.

Credit Cards

2. *The Board should adopt a written policy banning credit cards and credit lines if they do not intend that employees use them and ensure that District officials implement the policy. In addition, District officials should cancel any credit cards or credit lines that are not authorized.*

3. *If the Board plans to keep some or all of the credit cards, it should:*

- *Adopt a credit policy that addresses who is authorized to use the credit card, when, and how they can use the credit card and specify the documentation required.*
- *Ensure that District officials properly implement the policy.*
- *Ensure that District officials develop a credit card list documenting the number of cards, cardholders, and credit limits.*
- *Ensure that District officials develop a process for periodically reviewing authorized users and monitoring the use of existing cards.*

Corrective Action:

The Board is reconsidering a credit card policy.

If a credit card policy is enacted, procedures will be developed that will include periodically monitoring users and use.

If a credit card policy is enacted, authorization for credit cards and credit lines is required.

If a credit card policy is enacted, only authorized users will have access to use authorized credit cards.

The district has informed the issuers of unauthorized credit lines and credit card companies to cancel all prior existing credit lines and credit card accounts for the district.

4. The claims auditor should review each claim to ensure that it contains adequate documentation before approving payment.

5. The claims auditor should become familiar with the District purchasing and credit card policies and make sure that they are followed.

Corrective Action:

The claims auditor now provides detailed information of each approved claim voucher packet to the Board with her weekly report.

The claims auditor has access to all Board policies via the school district website. The district has instructed the Claims auditor to review the policies.

Information Technology

6. District officials should develop a formal, written, District-wide security plan.

7. The Board should periodically assess the risks resulting from outsourcing the District's IT services and take steps to ensure that appropriate controls are in place to minimize these risks.

8. The Director of Technology should institute a process to classify data according to the level of risk, document these classifications and ensure that appropriate controls are in place to address the risks.

9. District officials should develop and adopt comprehensive IT policies and procedures to address the physical security over its IT assets. Server room access should be monitored and restricted to authorized employees only.

10. District officials should develop policies and procedures to control and monitor remote access to financial computer data.

11. The Board and District officials should develop comprehensive written policies and procedures for the use of mobile storage devices such as flash drives.

12. The Board should adopt a written disaster recovery plan that addresses the potential loss of computer equipment and data. In addition, District officials should institute procedures for the recovery of data in the event that an actual loss occurs.

13. District officials should monitor user's access rights to ensure they are based on job functions and responsibilities, and promote proper segregation of duties.

14. District officials should adopt policies and procedures to establish user access controls that safeguard the District's computerized data and other IT assets. These controls should include a formal change process for authorizing, establishing, modifying, and promptly deactivating user access rights.

15. District officials should ensure there is a process for documenting software changes. This should include a record of authorizations, when changes were made, and who made the changes.

Corrective Action:

The Board of Education is reviewing policies in consideration of adoption to insure that financial networks, and all district systems, are adequately secured. The policy will address physical security over IT assets, remote access to computer data, the use of mobile storage devices, and a disaster recovery plan for equipment and data.

The district, through its insurance carrier, NYSIR, maintains computer fraud and loss coverage and may request a periodic assessment of risks associated with information technology.

The district implemented a new Financial Management System and Student Information System software with security and internal controls features. The district financial management system auto-generates auditing trails for each user and logs of all changes and edits on the system. These logs and trails provide immediate monitoring.

All mobile storage devices, including flash drives, purchased by the district are to be capable of encryption and password protection. This procedure is to be linked to the district security policy.

All user access rights to the financial and student information systems have been evaluated based on job functions and responsibilities to insure appropriate access as well as the segregation of duties.

The Director of Technology drafted a process by which to classify data and this document ensures appropriate controls and permissions based on user levels. These rights, as well as network access rights, are reviewed when created, as needed due to adjustments in an employee's job responsibilities and annually at the end of June. This is done collaboratively with the Human Resources department.

Entrance and Exit procedures for all positions in the district to include authorizing, establishing, modifying, and promptly deactivating user access rights have been established.

Files formerly held in the server room have been relocated and server room access is only available to the technology staff. The district is researching additional security measures at this location.

A disaster recovery plan for financial data is established and is tested with a disaster simulation annually. Network standards for disaster recovery include procedures for daily back up of network drives and off site storage of network files for security and safety.

A log of all software installs as well as software licenses are kept in the Technology office with the Director of Technology and the network engineer. Individual software installations are only performed by the district network engineer. The network is configured not to allow users rights to install personal or individual software.

The district network server has weekly updates. The server automatically logs the updates which are reviewed by the network engineer. The network engineer is notified via email as the updates occur and receives an "alert" with details of the update.