AUDITOR GENERAL

WILLIAM O. MONROE, CPA

POLK COUNTY DISTRICT SCHOOL BOARD
STUDENT ATTENDANCE SYSTEMS
Information Technology Audit

SUMMARY

The Polk County District School Board (District) utilized automated student grading and record-keeping systems to, among other things, record, edit, report, and track student attendance-related information. Our audit focused on evaluating selected information technology (IT) controls applicable to the student attendance systems during the period May 2006 through October 2006.

As described below, we noted that improvements were needed in certain controls over selected District IT functions and practices:

Finding No. 1: A comprehensive, written Districtwide information security program had not been devised to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls.

Finding No. 2: There was a need for improved District level governance of the student attendance systems.

BACKGROUND

The District's middle and high schools utilized Excelsior Software's Pinnacle System as their electronic student information management solution for integrating grade and administrative data. The District's use of Pinnacle, beginning in 1995-96, resulted from school-based initiatives in spending school-distributed Public School Technology Funds. While each school made the initial system purchase, in recent years, the District has provided 50% funding for purchasing additional modules. Additionally, the District paid the annual service contract cost to Excelsior for all District schools for both technical support as well as annual upgrade.

Within the Pinnacle System, the Gradebook2 module was used by teachers to electronically record student attendance. The Attendance Viewer module was used by each school's attendance clerk to modify or update student attendance based on a student's tardiness, excused absence, field trip, and other authorized absences from class. Attendance clerks' modifications automatically updated the teachers' files in the Pinnacle System and, through scheduled jobs, the Pinnacle System data was uploaded to the Genesis Student Information System (Genesis). Genesis served as the District's official record for student attendance.

The District operated the Pinnacle System under a decentralized model with each school housing its own system. Each school's Network Manager was designated as the local Pinnacle Administrator/Gradebook Manager for that school. System and security administration was performed through the Toolbox utility. In the fall of 2004, the District hired a full-time Systems Analyst as the District's Pinnacle Administrator to provide training and implementation support for the Pinnacle System. The District's Pinnacle Administrator maintained Pinnacle Administrator/Gradebook manager rights on all District schools' servers.

The District's elementary schools utilized EleGrade, an in-house developed application system integrated with Genesis. EleGrade was fully implemented during the 2004-05 school year. The Senior Programmer who developed the application, along with Help Desk staff, continued to provide support for the system. Through the EleGrade system, teachers recorded attendance and grades for their students. EleGrade attendance data was copied to the attendance table in Genesis to be available to users. Monitoring of attendance confirmation and update or modification was performed through the EleGrade Admin Viewer. Access to the Admin Viewer was designated by each school's principal. While each elementary teacher was responsible for taking his or her class attendance, the school's terminal operator or secretary may have been granted attendance related capabilities through the Admin Viewer.

The District's Information Systems and Technology Division (IST), under the direction of the Assistant Superintendent, IST, provided information technology services and support for District administration and schools, including management of the District's Wide Area Network infrastructure and configuration, operation of the data center, and installation and repair services for telecommunications equipment. IST staff maintained and administered the servers supporting Genesis. Both EleGrade and the Pinnacle System could be accessed through the District's network domain that is controlled by IST or through the school's local area network. The Pinnacle System provided Web-based access to student grade and attendance information for parents, students, teachers, and administrators. EleGrade provided Web-based access to student grade information for parents and teachers.

Our audit included a survey of designated school attendance personnel with administrative attendance update responsibilities from all schools under the direct authority of the District. We received and reviewed responses from 70 schools. Forty-six elementary schools provided responses related to attendance procedures and use of EleGrade. Twenty-four middle and high school attendance clerks provided responses related to procedures and use of the Pinnacle System Attendance Viewer. The results of the survey are summarized in Appendix A.

Finding No. 1: Districtwide Security Program

An entitywide program for information security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. Principles needed to ensure that the information security program addresses current risks include establishing a sound IT risk management process to identify, assess, and mitigate risks; implementing and communicating appropriate policies and controls; promoting security awareness; and monitoring the effectiveness of the policies and controls. Incorporating data classification into the entity's security program increases accountability for the integrity and security of data and enhances the effectiveness and control of sharing information.

Our audit disclosed the following deficiencies:

- Written policies and procedures for the student attendance systems had not been developed and incorporated into the District's security planning. Policies and procedures associated with effective security planning include delegation of authority for defining and enforcing policy for student attendance systems administration; identification, implementation, and monitoring of user access authorization and authentication controls and system control measures; and provision of a test environment for Pinnacle System upgrades.
- The District's on-going security awareness and training practices needed improvement. Typical means for establishing and maintaining awareness include informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality; distributing documentation describing security policies, procedures, and individual responsibilities; requiring users to periodically sign a statement acknowledging

their awareness and acceptance of responsibility; and requiring comprehensive security orientation, training and periodic refresher programs to communicate security guidelines to both new and existing employees. As part of the District's Information Security Awareness Plan, a list of security awareness facts emphasizing password protection practices was created and posted on the IST Web site. Additionally, this list of security tips was e-mailed to all staff on a monthly basis with a request to consider these in keeping the network secure. Staff were not required to acknowledge they had received, understood, and agreed to abide by the practices. Further, Network Managers were reminded of the importance of security awareness and requested to share information with school staff, including during application training. Responses to Question 11 of our audit survey disclosed inconsistencies regarding awareness of, and attendance at Pinnacle and EleGrade training sessions and whether the content included coverage of security awareness issues.

- The District did not enforce, through automated means, or monitor provisions of Board Policy (6Gx53-9.001) prohibiting installation of personally-owned software without prior approval of the appropriate school or District technology personnel. During our audit, we noted that users maintained local administrator rights to their individual workstations, thereby allowing installation of personal software without prior approval and evidence of valid software license(s).
- Board Policy (6Gx53-9.006) stated that sensitive or confidential data may only be transferred across networks or copied to other media when the confidentiality and integrity of the data can be reasonably assured. The District had not developed written standards for the classification of data, including student data, based on its level of sensitivity to reasonably ensure that the confidentiality and integrity of the data was maintained outside the District's supported systems.
- The District had not documented, in the form of written policies, that sound business practices had been established for authorizing and securing user accounts for network, host operating system, and database administration, including defining personnel to these accounts based on appropriate job responsibilities and password management procedures.
- The District did not have a mechanism for imposing and monitoring compliance with Board policy (6Gx53-9.005) regarding controlling physical access to designated high security areas. Specifically, measures were not in place to ensure that physical access to student attendance system servers and network component equipment at each school site facility was adequately controlled.
- The District had not performed a comprehensive risk assessment of its network, including assessment specific to the student attendance systems. Risk management is the process of identifying vulnerabilities and threats to IT resources used in achieving business objectives, and deciding what measures, if any, to take in reducing risk to an acceptable level. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.
- Although available in the software, certain important security features for user identification and authentication, workstation controls, and user access had either not been utilized or were inadequate to protect the network and the administrative applications. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.

While the Board had defined overall policies for the District as noted above, these policies had not been applied through detailed and enforceable written procedures developed as part of a comprehensive, written information security program. The absence of a security program limits the District's ability to formulate and implement sound management policies designed to affect a secure processing environment in support of the District's intended mission and responsibilities to its students and user community. Further, without an adequate security awareness program for all staff with access to IT resources, the risk is increased that employees may not be aware of their security responsibilities or the consequences of not fulfilling those responsibilities.

Recommendation: The District should develop a comprehensive, written Districtwide security program, along with corresponding policies and procedures, describing management's expectations regarding IT risk management and security controls.

Finding No. 2: District Governance of the Student Attendance Systems

Management strategies for shared information resources and systems must be coordinated across the enterprise. Allowing department or division-level segments of the enterprise to make decisions in isolation from others is likely to result in an inefficient and ineffective strategy for increasing accountability for the integrity and security of the enterprise system and data contained therein. Ensuring that enterprise policies are distributed to staff and enforced enable those policies to be built into and become an integral part of operations. Further, continuous evaluation of compliance with policies, standards, and procedures based on management's governance oversight and operation of internal controls identifies compliance gaps in order to timely respond with corrective action.

Our audit disclosed the following deficiencies:

- ➢ While the District Pinnacle Administrator provides recommendations and instruction during training, the District had not established written guidelines, policies, or procedures for the Pinnacle System, including architecture standards and installation schema; granting system administrator rights through Toolbox utility access; authorizing and reviewing user access to critical system folders, class files, and component modules; and requiring all attendance updates or modifications to be done through the Attendance Viewer module. Additionally, each school principal and vice-principal were pre-authorized for access to the EleGrade Admin Viewer with authority to grant full access rights to the Admin Viewer to up to five additional personnel. However, the District had not established written policies for granting access to the EleGrade Admin Viewer, including provisions that authorizing administrative level access should be based on defined job responsibility to prevent excessive or unnecessary access from being granted.

- ➢ Our review of survey responses disclosed a lack of consistent application of procedures in utilizing student attendance systems in association with student attendance mandates. While some commonality existed among the functions of and tools used by the attendance personnel, respondents indicated that with regard to their responsibilities and the use of Pinnacle or EleGrade, they followed District-developed, school-developed, or personally-developed policies and procedures or expressed that there were no written policies and procedures related to their job responsibilities. (See Appendix A, Question 5.) Specifically, policies and procedures were lacking or needed improvement in the following areas:

  - Respondents indicated varied use and review of attendance monitoring reports to ensure teacher input of attendance as appropriate. The District's Pinnacle Administrator recommended that attendance tracking reports be run daily to list those teachers who did not take attendance the previous day in support of the Florida Department of Education's policy that daily sign-ons, indicating attendance had been taken, be reported by exception and reviewed on a regular basis. However, there was no written or enforced District policy for this. Neither was there a Districtwide escalation procedure for those teachers who repeatedly did not complete attendance-taking in the appropriate timeframe given.

  - The District had not defined reconciliation procedures between Pinnacle and Genesis to ensure the complete and appropriate update of attendance data to Genesis.

  - The District had not developed and distributed written policies and procedures regarding maintenance of hard copy documentation supporting changes made in student attendance records. Further, the District had not established standards for notating the basis for attendance changes made within the Pinnacle and EleGrade application systems through available comment fields.

- The District followed a "train the trainer" methodology whereby District Pinnacle and EleGrade Administrators trained the Network Managers, who, in turn, would train school staff on the attendance systems. Additionally, the District Pinnacle Administrator provided training on the Attendance Viewer module to the schools' attendance clerks. However, survey responses indicated that not all attendance personnel attended training or were aware of training. (See Appendix A, Question 11.)
- The District did not have procedures in place for controlling user access to the student attendance systems to ensure best practice guidelines are followed in accordance with Board policy (6Gx53-9.005). We noted instances where survey respondents indicated that their designated back-up had not been assigned a unique user ID and password. (See Appendix A, Question 13.)

These deficiencies indicate a need for improved District-level governance of the student attendance systems and the data contained therein, including standardized procedures and centralized enforcement. The absence of District-initiated policies and procedures lessens the District's assurance of the effective use of the student attendance systems and the integrity of the data contained therein.

Recommendation: The District should examine the human and system elements of the attendance-taking functions; identify potential errors or misuse associated with recording student attendance; and establish controls, particularly in the aforementioned areas, to promote data accuracy and integrity. To ensure consistent application among all school sites, the District should establish written Districtwide policies and procedures that document management's expectations regarding controls over attendance data integrity.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application IT controls applicable to the student attendance systems. Our scope focused on evaluating these selected controls during the period May 2006 through October 2006. In conducting our audit, we interviewed appropriated District personnel, surveyed selected school personnel, reviewed District processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated December 14, 2006, the Superintendent provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix B.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Heidi Burns, CPA*, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A

School Attendance Personnel Survey Results

In an effort to determine whether the District had developed policies and procedures designed to promote the integrity of student attendance data through the adequate and consistent utilization of Pinnacle and EleGrade, we conducted a survey of all schools under the direct authority of the District. At the time of our survey, May 17, 2006, the number of schools included 61 elementary schools and 34 middle and high schools, for a total of 95 surveys. The survey was electronically sent to each school's principal with a request for a response from the school's designated attendance clerk or other individual who was assigned attendance-related administrative update functions. A total of 70 schools responded representing 46 elementary schools and 24 middle and high schools. Our tabulation of the responses to the survey questions follows:

1. and 2. Questions 1 and 2 asked for identification information regarding the school and person completing the survey.

3. Question 3 asked about availability during the summer months for any questions.

4. Question 4 asked the clerk to list any responsibilities in addition to attendance.

5. With regard to the attendance clerk responsibilities and use of the student attendance system, please indicate by inserting an 'X' which statement is true.
___ The District developed and distributed formal written policies and procedures.
___ I follow the formal written policies and procedures developed by my individual school.
___ I have developed my own written policies and procedures.
___ There are no formal written policies and procedures for the use of the system as it relates to my job responsibilities.

Response	EleGrade	%*	Pinnacle	%*
The District developed and distributed formal written policies and procedures.	20	43%	7	29%
I follow the formal written policies and procedures developed by my individual school.	7	15%	6	25%
I have developed my own written policies and procedures.	1	2%	0	0%
Combination of District developed policies, school policies, and/or own policies.	7	15%	7	29%
There are no formal written policies and procedures for the use of the system as it relates to my job responsibilities.	5	11%	3	13%
No Response	6	13%	1	4%

6. Please indicate by inserting a '√' which of the following statements are true and complete the sentence where highlighted, as appropriate.
___ I run and review attendance monitoring reports at __________ intervals.
___ I do not utilize attendance monitoring reports.
___ A defined policy requires monitoring reports to be run and reviewed on a daily basis.
___ The policy is District-based.
___ The policy is school-based.

Response	EleGrade	%*	Pinnacle	%*
I run and review attendance monitoring reports at **Daily** intervals.	8	17%	16	67%
I run and review attendance monitoring reports at **Weekly** intervals.	18	39%	2	8%
I run and review attendance monitoring reports at **twice Monthly** intervals.	0	0%	1	4%
I run and review attendance monitoring reports at **Monthly** intervals.	6	13%	0	0%
I run and review attendance monitoring reports at **Specific times or Hourly** intervals.	0	0%	1	4%
I run and review attendance monitoring reports at **Regular** intervals.	1	2%	1	4%
I run and review attendance monitoring reports **As Needed.**	2	4%	1	4%
I run and review attendance monitoring reports at **9 week** intervals.	2	4%	0	0%
I run and review attendance monitoring reports per **FTE.**	1	2%	0	0%
No Interval Provided	5	11%	1	4%
No Response	3	7%	1	4%

Responses regarding the existence of policy varied, ranging from no indication of a policy to both a defined District and school-based policy.

7. For each day's/period's attendance, please describe your follow-up procedures for those teachers who have not taken the required attendance.

   Responses varied by school regarding follow-up procedures and included verbal communication to the teacher, written communication to the teacher, or no follow-up procedures in place.

8. Please describe any escalation procedures that are performed for those teachers who repeatedly do not complete attendance taking requirements within the appropriate timeframe given.

   Responses varied by school regarding escalation procedures and included having direct communication with the teacher, involving school administration for formal and informal disciplinary actions, or having no escalation procedures in place. Eight schools indicated this is not an issue at the school.

9. Please provide a brief explanation of reconciliation procedures performed between the student attendance system data and the official student record with regard to attendance.

   This question focused on procedures or standard reports in place to ensure the accurate update of the Genesis database by the nightly FTP process of Pinnacle data. Responses varied by the high schools with four attendance clerks indicating that some measures existed to review for discrepancies in the attendance records. However, use of a standard report to verify the nightly upload was not indicated.

10. Please indicate by inserting a '√' which of the following statements are true.
    ___ Back-up documentation (i.e., notes) for changes in student attendance reporting are filed and maintained.
    ___ Changes made to the attendance record are notated through the use of a comment field in the system.
    ___ Back-up documentation is not maintained.
    ___ Comment fields are available, but not used.
    ___ District policy states back-up documentation will be maintained.
    ___ School policy states back-up documentation will be maintained.
    ___ District policy requires completion of comment fields.
    ___ School policy requires completion of comment fields.

Response	**EleGrade**	**%***	**Pinnacle**	**%***
Back-up documentation (i.e., notes) for changes in student attendance reporting are filed and maintained.	32	70%	9	38%
Back-up documentation (i.e., notes) for changes in student attendance reporting are filed and maintained; Changes made to the attendance record are notated through the use of a comment field in the system.	2	4%	10	42%
Changes made to the attendance record are notated through the use of a comment field in the system	1	2%	2	8%
Back-up documentation is not maintained.	1	2%	0	0%
Comment fields are available, but not used.	1	2%	1	4%
Response Inconclusive	1	2%	1	4%
No Response	8	17%	1	4%

Responses regarding the existence of policy varied, ranging from no indication of a policy to both a defined District and school-based policy.

11. Please indicate by inserting a '√' which of the following statements are true and complete the sentence where highlighted, as appropriate.
    ___ I attended Attendance Clerk training for the student attendance system on _______________.
    ___ My designated back-up attended training for the student attendance system on ______________.
    ___ Attendance Clerk training was not provided for the student attendance system.
    ___ Training included discussion of security awareness issues.

Response	**EleGrade**	**%***	**Pinnacle**	**%***
I attended Attendance Clerk training for the student attendance system; My designated back-up attended training for the student attendance system.	2	4%	5	21%
I attended Attendance Clerk training for the student attendance system; My designated back-up attended training for the student attendance system; Training included discussion of security awareness issues.	2	4%	6	25%
I attended Attendance Clerk training for the student attendance system.	3	7%	1	4%
I attended Attendance Clerk training for the student attendance system; Training included discussion of security awareness issues.	4	9%	2	8%
My designated back-up attended training for the student attendance system and/or Training included discussion of security awareness issues; No Indication of own attendance.	4	9%	0	0%
Attendance Clerk training was not provided for the student attendance system or unaware of training.	19	41%	6	25%
No Response or Not Applicable	12	26%	4	17%

12. Question 12 asked the clerk to complete information related to password controls. Specific details of the responses are not disclosed here to avoid the possibility of compromising District information. However, as referenced in the final bullet of Finding No. 1, appropriate District personnel have been notified of the related issue.

13. Please indicate by inserting an 'X' whether the individual(s) designated as a back-up is assigned his/her own ID and password for the system.
    ___ Yes
    ___ No

Response	EleGrade	%*	Pinnacle	%*
Yes	27	59%	17	71%
No	6	13%	2	8%
No Response	11	24%	4	17%
Not Applicable (No Attendance Clerk)	2	4%	1	4%

14. Question 14 asked the clerk to complete information related to workstation settings. Specific details of the responses are not disclosed here to avoid the possibility of compromising District information. However, as referenced in the final bullet of Finding No. 1, appropriate District personnel have been notified of the related issue.

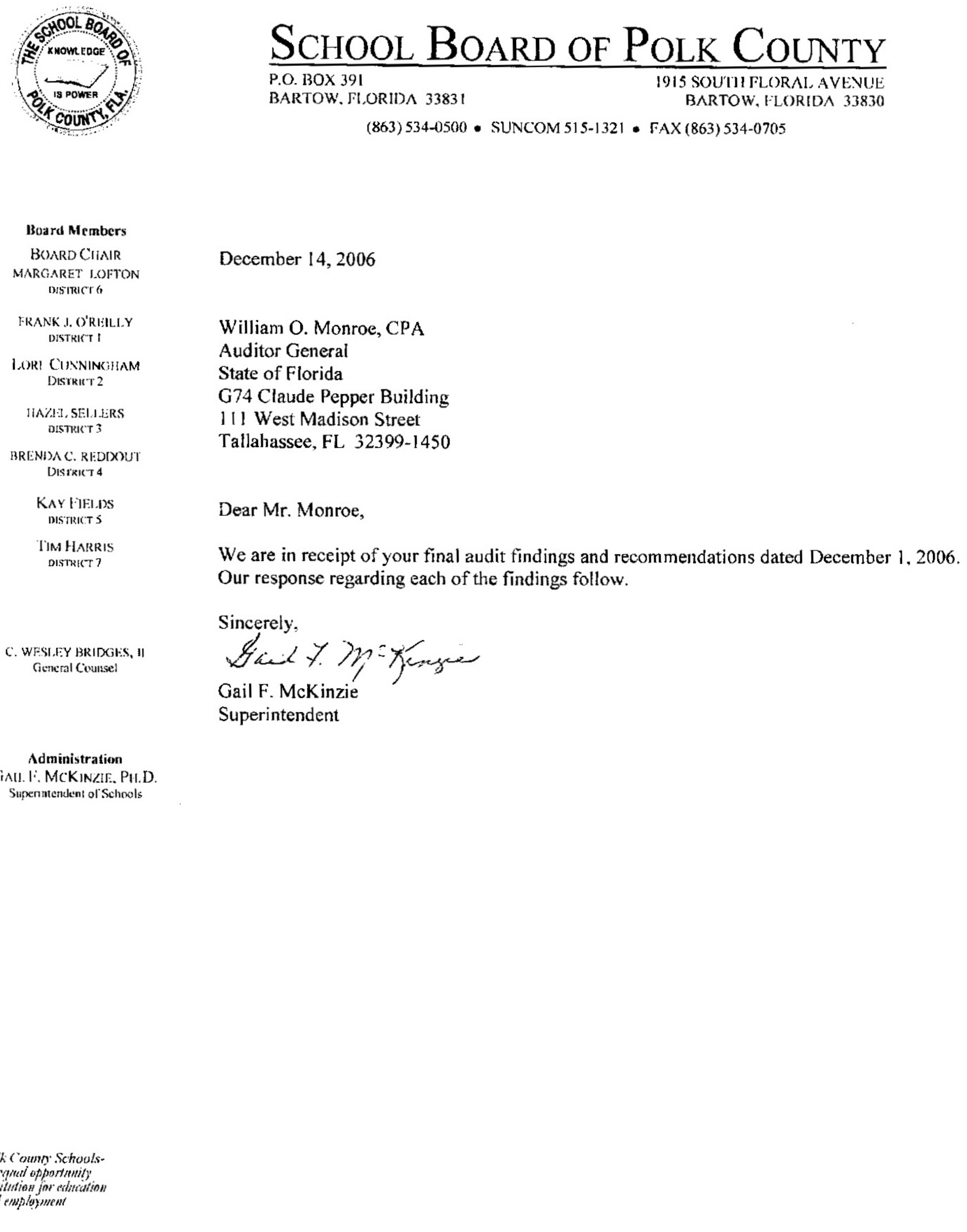
15. If you would like to provide any other comments/information, please do so here. If a comment relates to a particular question, please indicate the question number before the comment.

    Of the general comments provided, four pertained to lack of knowledge whether training classes were available, desire for attendance training courses and written guidelines to follow, system problems, and the inability to access attendance reports from Genesis.

    * Percentages are shown rounded to the nearest whole number.

APPENDIX B

MANAGEMENT RESPONSE



SCHOOL BOARD OF POLK COUNTY

P.O. BOX 391
BARTOW, FLORIDA 33831

1915 SOUTH FLORAL AVENUE
BARTOW, FLORIDA 33830

(863) 534-0500 • SUNCOM 515-1321 • FAX (863) 534-0705

Board Members

BOARD CHAIR
MARGARET LOFTON
DISTRICT 6

FRANK J. O'REILLY
DISTRICT 1

LORI CUNNINGHAM
DISTRICT 2

HAZEL SELLERS
DISTRICT 3

BRENDA C. REDDOUT
DISTRICT 4

KAY FIELDS
DISTRICT 5

TIM HARRIS
DISTRICT 7

C. WESLEY BRIDGES, II
General Counsel

Administration
GAIL F. MCKINZIE, PH.D.
Superintendent of Schools

*Polk County Schools-
an equal opportunity
institution for education
and employment*

December 14, 2006

William O. Monroe, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

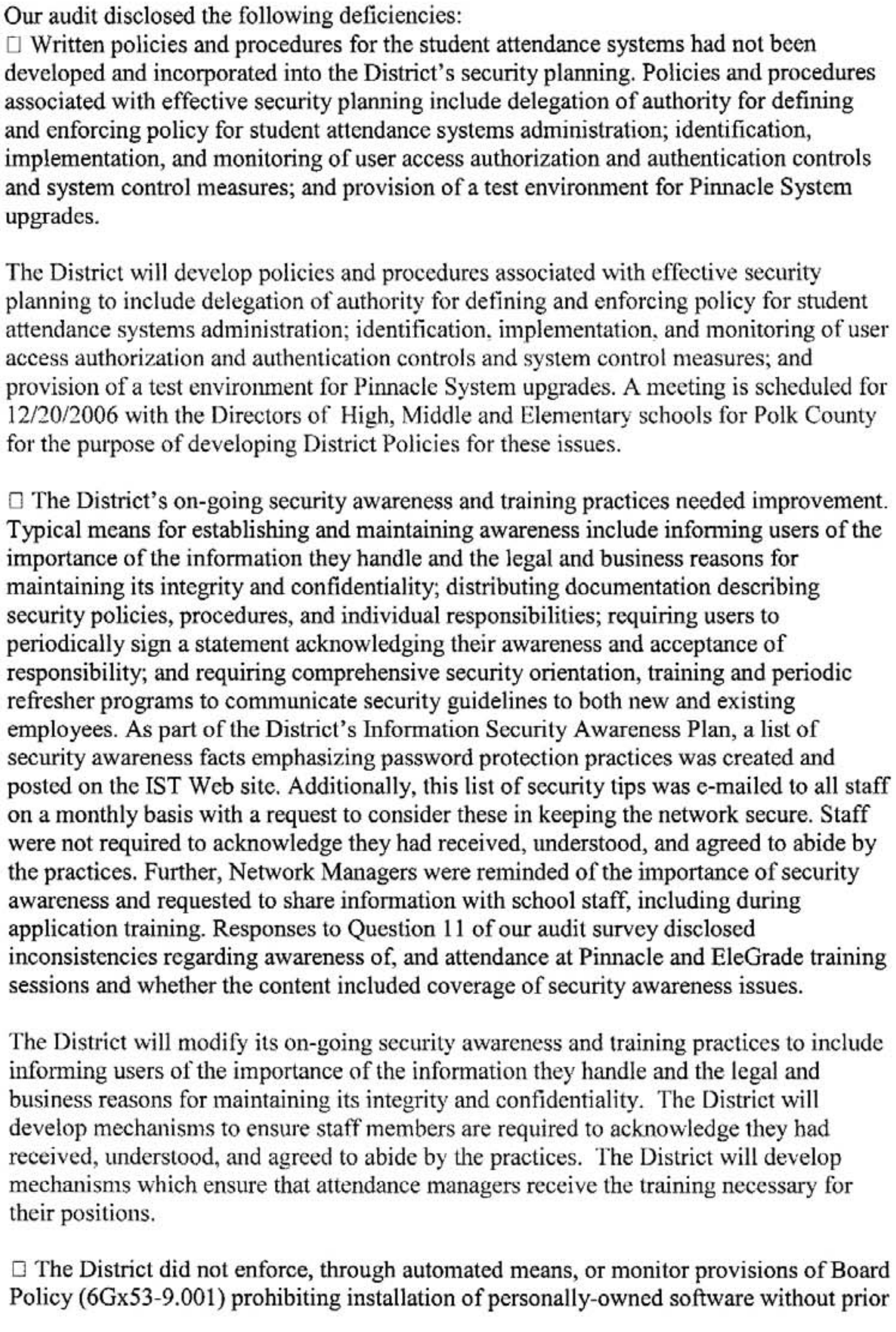
Dear Mr. Monroe,

We are in receipt of your final audit findings and recommendations dated December 1, 2006. Our response regarding each of the findings follow.

Sincerely,

Gail F. McKinzie

Gail F. McKinzie
Superintendent



Our audit disclosed the following deficiencies:

□ Written policies and procedures for the student attendance systems had not been developed and incorporated into the District's security planning. Policies and procedures associated with effective security planning include delegation of authority for defining and enforcing policy for student attendance systems administration; identification, implementation, and monitoring of user access authorization and authentication controls and system control measures; and provision of a test environment for Pinnacle System upgrades.

The District will develop policies and procedures associated with effective security planning to include delegation of authority for defining and enforcing policy for student attendance systems administration; identification, implementation, and monitoring of user access authorization and authentication controls and system control measures; and provision of a test environment for Pinnacle System upgrades. A meeting is scheduled for 12/20/2006 with the Directors of High, Middle and Elementary schools for Polk County for the purpose of developing District Policies for these issues.

□ The District's on-going security awareness and training practices needed improvement. Typical means for establishing and maintaining awareness include informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality; distributing documentation describing security policies, procedures, and individual responsibilities; requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility; and requiring comprehensive security orientation, training and periodic refresher programs to communicate security guidelines to both new and existing employees. As part of the District's Information Security Awareness Plan, a list of security awareness facts emphasizing password protection practices was created and posted on the IST Web site. Additionally, this list of security tips was e-mailed to all staff on a monthly basis with a request to consider these in keeping the network secure. Staff were not required to acknowledge they had received, understood, and agreed to abide by the practices. Further, Network Managers were reminded of the importance of security awareness and requested to share information with school staff, including during application training. Responses to Question 11 of our audit survey disclosed inconsistencies regarding awareness of, and attendance at Pinnacle and EleGrade training sessions and whether the content included coverage of security awareness issues.

The District will modify its on-going security awareness and training practices to include informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality. The District will develop mechanisms to ensure staff members are required to acknowledge they had received, understood, and agreed to abide by the practices. The District will develop mechanisms which ensure that attendance managers receive the training necessary for their positions.

□ The District did not enforce, through automated means, or monitor provisions of Board Policy (6Gx53-9.001) prohibiting installation of personally-owned software without prior approval of the appropriate school or District technology personnel. During our audit, we noted that users maintained local administrator rights to their individual workstations, thereby allowing installation of personal software without prior approval and evidence of valid software license(s).

As part of the implementation of district-wide Active Directory and a Desktop Management System over a 2 year period, this will be addressed.

□ Board Policy (6Gx53-9.006) stated that sensitive or confidential data may only be transferred across networks or copied to other media when the confidentiality and integrity of the data can be reasonably assured. The District had not developed written standards for the classification of data, including student data, based on its level of sensitivity to reasonably ensure that the confidentiality and integrity of the data was maintained outside the District's supported systems.

The District will develop written standards for the classification of data, including student data, based on its level of sensitivity to reasonably ensure that the confidentiality and integrity of the data is maintained outside the District's supported systems.

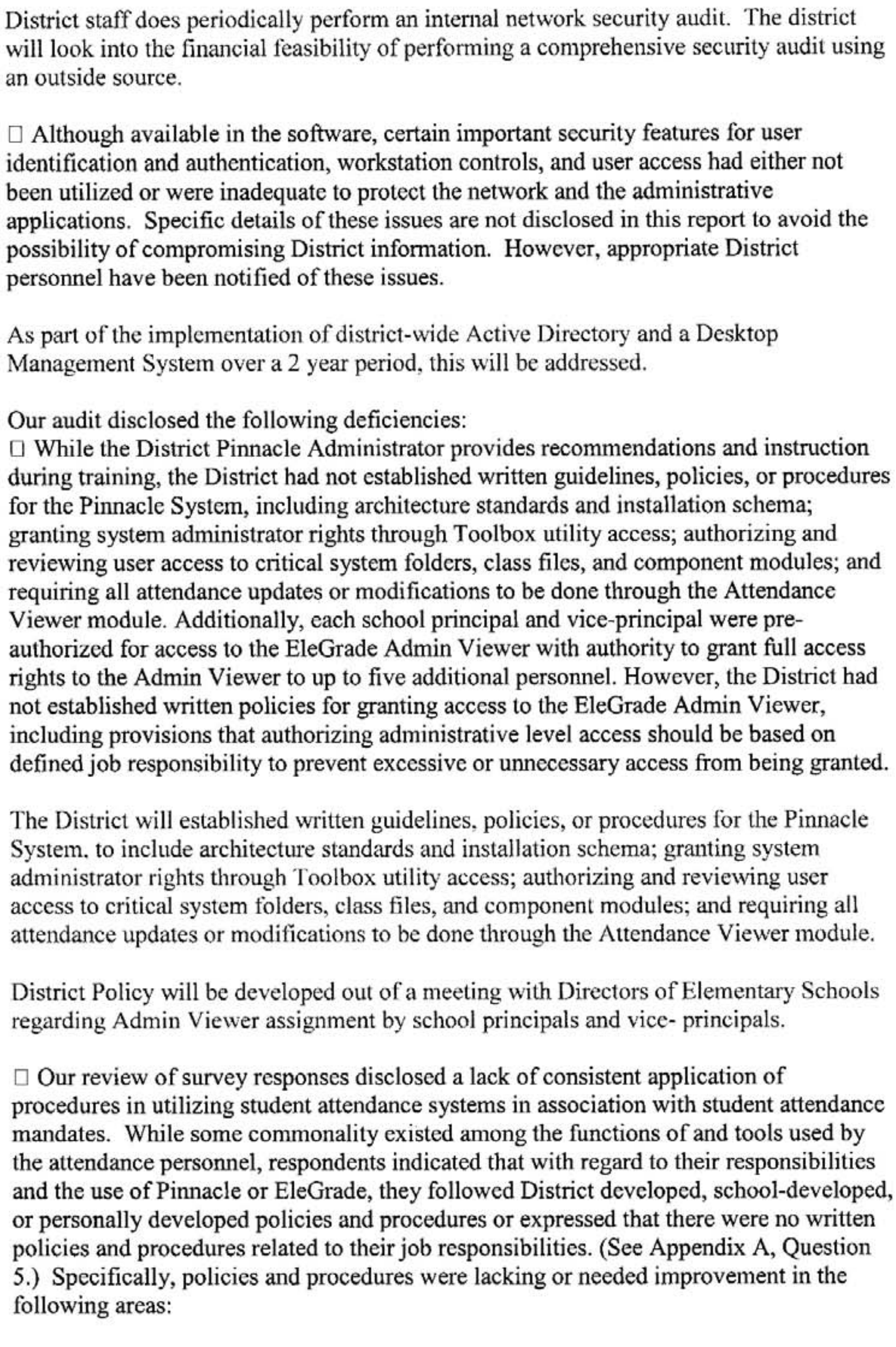
□ The District had not documented, in the form of written policies, that sound business practices had been established for authorizing and securing user accounts for network, host operating system, and database administration, including defining personnel to these accounts based on appropriate job responsibilities and password management procedures.

District will review existing policies and implement policies and procedures to address this point.

□ The District did not have a mechanism for imposing and monitoring compliance with Board policy (6Gx53-9.005) regarding controlling physical access to designated high security areas. Specifically, measures were not in place to ensure that physical access to student attendance system servers and network component equipment at each school site facility was adequately controlled.

The IST Division will work with the Facilities Division to establish physical security of network and server resources as funding is made available.

□ The District had not performed a comprehensive risk assessment of its network, including assessment specific to the student attendance systems. Risk management is the process of identifying vulnerabilities and threats to IT resources used in achieving business objectives, and deciding what measures, if any, to take in reducing risk to an acceptable level. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.



District staff does periodically perform an internal network security audit. The district will look into the financial feasibility of performing a comprehensive security audit using an outside source.

□ Although available in the software, certain important security features for user identification and authentication, workstation controls, and user access had either not been utilized or were inadequate to protect the network and the administrative applications. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.

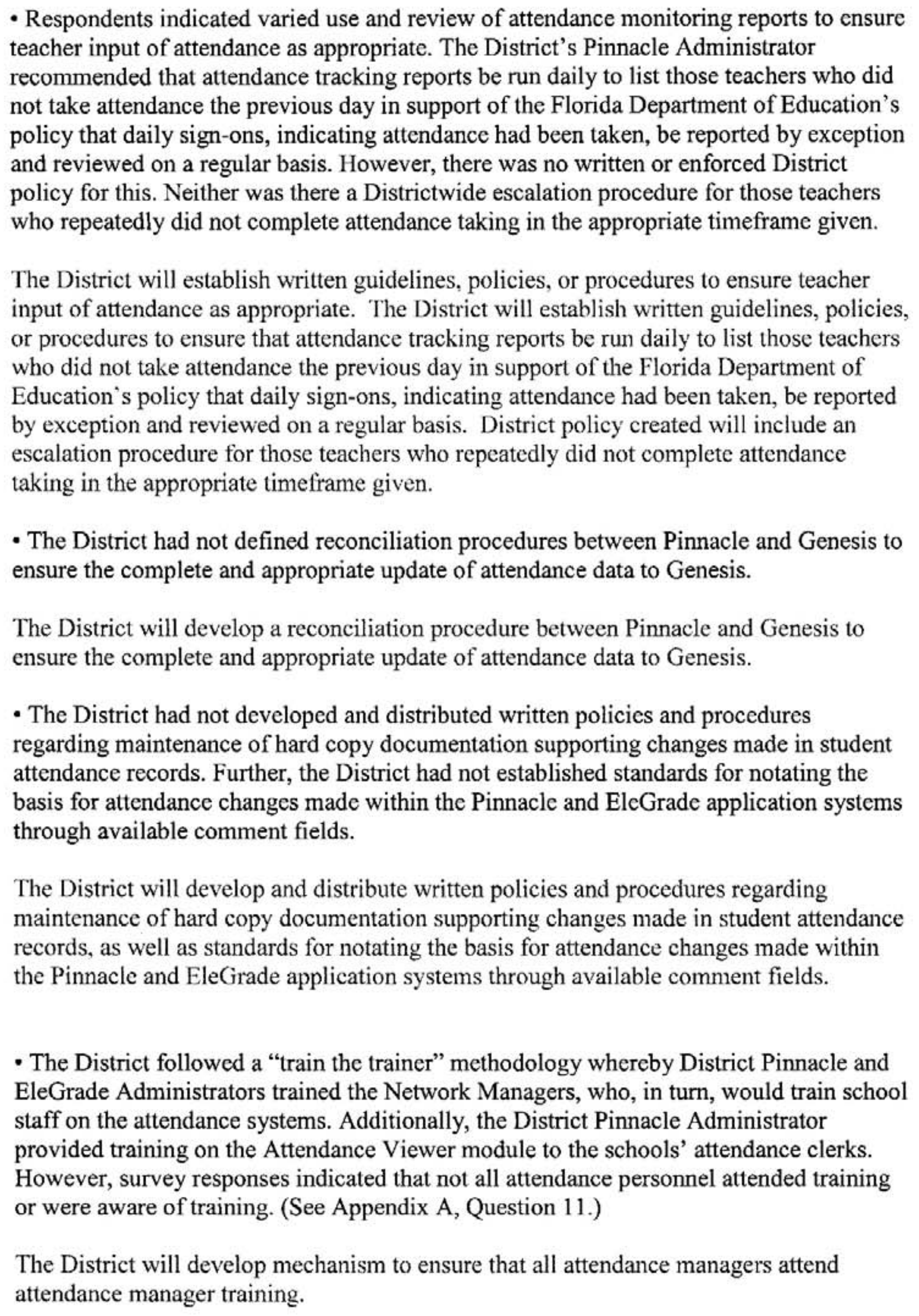
As part of the implementation of district-wide Active Directory and a Desktop Management System over a 2 year period, this will be addressed.

Our audit disclosed the following deficiencies:
□ While the District Pinnacle Administrator provides recommendations and instruction during training, the District had not established written guidelines, policies, or procedures for the Pinnacle System, including architecture standards and installation schema; granting system administrator rights through Toolbox utility access; authorizing and reviewing user access to critical system folders, class files, and component modules; and requiring all attendance updates or modifications to be done through the Attendance Viewer module. Additionally, each school principal and vice-principal were pre-authorized for access to the EleGrade Admin Viewer with authority to grant full access rights to the Admin Viewer to up to five additional personnel. However, the District had not established written policies for granting access to the EleGrade Admin Viewer, including provisions that authorizing administrative level access should be based on defined job responsibility to prevent excessive or unnecessary access from being granted.

The District will established written guidelines, policies, or procedures for the Pinnacle System, to include architecture standards and installation schema; granting system administrator rights through Toolbox utility access; authorizing and reviewing user access to critical system folders, class files, and component modules; and requiring all attendance updates or modifications to be done through the Attendance Viewer module.

District Policy will be developed out of a meeting with Directors of Elementary Schools regarding Admin Viewer assignment by school principals and vice- principals.

□ Our review of survey responses disclosed a lack of consistent application of procedures in utilizing student attendance systems in association with student attendance mandates. While some commonality existed among the functions of and tools used by the attendance personnel, respondents indicated that with regard to their responsibilities and the use of Pinnacle or EleGrade, they followed District developed, school-developed, or personally developed policies and procedures or expressed that there were no written policies and procedures related to their job responsibilities. (See Appendix A, Question 5.) Specifically, policies and procedures were lacking or needed improvement in the following areas:



- Respondents indicated varied use and review of attendance monitoring reports to ensure teacher input of attendance as appropriate. The District's Pinnacle Administrator recommended that attendance tracking reports be run daily to list those teachers who did not take attendance the previous day in support of the Florida Department of Education's policy that daily sign-ons, indicating attendance had been taken, be reported by exception and reviewed on a regular basis. However, there was no written or enforced District policy for this. Neither was there a Districtwide escalation procedure for those teachers who repeatedly did not complete attendance taking in the appropriate timeframe given.

The District will establish written guidelines, policies, or procedures to ensure teacher input of attendance as appropriate. The District will establish written guidelines, policies, or procedures to ensure that attendance tracking reports be run daily to list those teachers who did not take attendance the previous day in support of the Florida Department of Education's policy that daily sign-ons, indicating attendance had been taken, be reported by exception and reviewed on a regular basis. District policy created will include an escalation procedure for those teachers who repeatedly did not complete attendance taking in the appropriate timeframe given.

- The District had not defined reconciliation procedures between Pinnacle and Genesis to ensure the complete and appropriate update of attendance data to Genesis.

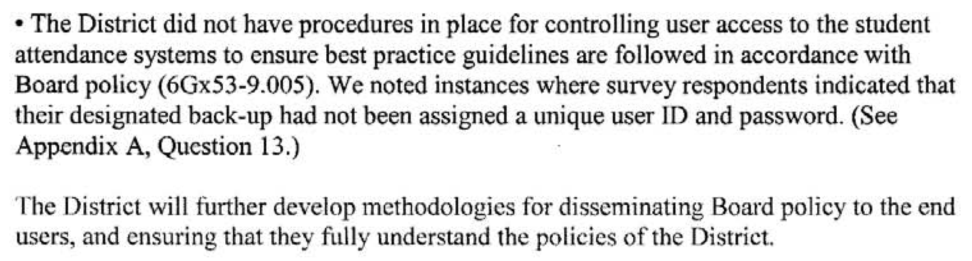
The District will develop a reconciliation procedure between Pinnacle and Genesis to ensure the complete and appropriate update of attendance data to Genesis.

- The District had not developed and distributed written policies and procedures regarding maintenance of hard copy documentation supporting changes made in student attendance records. Further, the District had not established standards for notating the basis for attendance changes made within the Pinnacle and EleGrade application systems through available comment fields.

The District will develop and distribute written policies and procedures regarding maintenance of hard copy documentation supporting changes made in student attendance records, as well as standards for notating the basis for attendance changes made within the Pinnacle and EleGrade application systems through available comment fields.

- The District followed a "train the trainer" methodology whereby District Pinnacle and EleGrade Administrators trained the Network Managers, who, in turn, would train school staff on the attendance systems. Additionally, the District Pinnacle Administrator provided training on the Attendance Viewer module to the schools' attendance clerks. However, survey responses indicated that not all attendance personnel attended training or were aware of training. (See Appendix A, Question 11.)

The District will develop mechanism to ensure that all attendance managers attend attendance manager training.



• The District did not have procedures in place for controlling user access to the student attendance systems to ensure best practice guidelines are followed in accordance with Board policy (6Gx53-9.005). We noted instances where survey respondents indicated that their designated back-up had not been assigned a unique user ID and password. (See Appendix A, Question 13.)

The District will further develop methodologies for disseminating Board policy to the end users, and ensuring that they fully understand the policies of the District.