June 14, 2010

Denver McClendon, Chairman
Robert Zárate, ABF Committee Chairman
Board of Trustees
Alamo Colleges
201 W. Sheridan
San Antonio, Texas 78204

Dear Mr. McClendon, Mr. Zárate and Trustees

Re: Student Information System Plus Security Processes and Controls Review Reports

Alamo Colleges Internal Audit Department completed a review of the Student Information System Plus (SIS Plus) Security Processes and Controls. This was the second of several student financial services projects included in the Approved Internal Audit Plan for Fiscal Year 2009. A report for the first phase, which was a performance review of the Student Financial Services Department, was issued in May. Other phases planned included reviews of student transactions processed and financial aid awards. At this time, field work continues on the transaction and awards analyses with completion anticipated during the summer.

Student services are the focal point of the District’s strategic plan. Each year, Alamo Colleges receives over $100 million in financial aid to award and disburse to students. In addition, student fees and charges assessed account for over $50 million in annual revenue. Millions of nonfinancial records, such as registration and grades, are processed annually for more than 60,000 students attending Alamo Colleges.

For over twenty years, the District has used a centralized Mainframe application known as SIS Plus to process these records for the five separate databases that have been configured to accommodate the campuses. The District has used the Series Z Security Software in conjunction with the student application to manage operator access. Using the applications’ functionality, Operator Identifier Codes (Operator IDs) are established with access only, inquiry only, or a combination of privileges. In addition, password controls are used to manage the 2,600 plus active Operator IDs.

Enclosed are the final reports for the Student Information System Plus Security Processes and Controls Review which includes an executive summary and a more detailed report with related appendices. This report documents twenty-six unique recommendations to enhance controls and to improve compliance with federal requirements and with District’s policies/procedures. Attached for your convenience is a copy of Alamo Colleges Management Responses to the audit recommendations. This effort was recently coordinated by the Vice Chancellor for Finance and Administration.
In the past, it does not appear that Management has adequately understood the various risks involved with using information systems to process, report and maintain student related data. This conclusion was due in part to the lack of monitoring and information reports for Operator access and transactions. Management has probably assumed that the processes/procedures were adequate, and that the applications' functions and controls were effectively used. Further, Management may have believed that several District or College Departments were appropriately monitoring transaction processing. Regardless of the reasons, control weaknesses increase the District's risks and the possible exposure to fraud, abuse and/or errors in processing student data.

Critical resource allocation decisions for student system security and controls may not have evaluated all of the major risks in conjunction with an appropriate cost-benefit analysis. Adequately addressing these risks is critical if Alamo Colleges is to successfully achieve the administrative capability standards required by federal regulations for entities handling student financial aid. The District must also ensure the adequacy of resources to comply with the Texas Administrative Code Section 202 Information Security Standards and with the Board's policies.

Alamo Colleges Management has expressed concerns about using limited resources to remediate the control deficiencies noted for the SIS Plus and Series Z Security Applications. Internal Audit acknowledges their concerns; however, we strongly encourage Management to ensure that the Banner Student and Financial Aid Modules Implementation resolve the most significant security gaps documented. If front-end preventive controls are not possible then meaningful exception reports can be used as back-end detection alternatives. However, specific personnel must be assigned responsibility and accountability to review them in a timely manner, and to report irregularities to Management immediately. In addition, these individuals must be properly trained on how to use these reporting tools.

It should be noted that several of the security and access concerns documented and reported to Management are not new. In spring 2009, Internal Audit issued a report regarding a St. Philip's College employee which indicated similar student information system security and/or control issues. In fall 2009, the Texas State Auditor's Office reported to the Alamo Colleges that the student system used by Northwest Vista College needed improved security. In fall 2008, the Denim Group reported to the District several high-level information technology security risk issues that have previously been shared with the Board.

In 2003, the Texas Comptroller's Report on the Performance Review of the Alamo Community College District included over one-hundred recommendations. Among them was a suggestion to hire a Chief Information Officer. As of spring 2008, the District Director for Information Technology Services (ITS) has been given this designation. This report also recommended consolidating the college information technology departments with the District ITS Department. This consolidation was recommended to streamline the functions, to implement a more service oriented organization, and to eliminate duplicate positions. To date, this has not occurred.
This message about improving student information security is not new. The emphasis has been significantly shifting in recent years due to technology advances. During these times of financial constraints, Alamo Colleges Management and the Board should ensure that sufficient resources are allocated for data security, especially student electronic and paper records. Past experience indicates that this has not been adequately funded.

We are available to discuss with you individually any of the information provided or to respond to any questions that you might have about this project. Internal Audit thanks the Board of Trustees for its continued support of our activities.

Sincerely,

Patricia M. Major CPA, CIA, CGAP  
District Director of Internal Audit

Attachments: 3

cc: Dr. Bruce Leslie, Chancellor  
  Ms. Diane Snyder, Vice Chancellor for Finance & Administration  
  Dr. Adelina Silva, Vice Chancellor for Student Success  
  Dr. Thomas Cleary, Vice Chancellor for Planning, Performance & Information Systems  
  Ms. Linda Boyer-Owens, Associate Vice Chancellor for Human Resources  
  Mr. Richard Hernandez, District Director of Student Financial Services  
  Mr. Roger Castro, District Director of Information Technology Services  
  Mr. Erik Dahler, District General Counsel  
  Ms. Pamela Ansboury, Associate Vice Chancellor for Finance & Fiscal Services
Student Information System Plus Security
Processes and Controls Review
Executive Summary
July 31, 2009

Prepared by: Alamo Colleges Internal Audit Department
Patricia M. Major CPA, CIA, CGAP, CTP, CGFM
Francisco Cortez CIA, CISA, CISSP
Oscar T. Salazar CISA, CISSP
Leticia T. Charbonneau CPA
Rosaura Ramirez CPA, CIA, CTP
Cynthia Munoz
## TABLE OF CONTENTS – EXECUTIVE SUMMARY

<table>
<thead>
<tr>
<th>Description</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>ES 1</td>
</tr>
<tr>
<td>Scope and Methodology</td>
<td>ES 3</td>
</tr>
<tr>
<td>Statement of Auditing Standards</td>
<td>ES 4</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>ES 4</td>
</tr>
<tr>
<td>Objectives</td>
<td>ES 5</td>
</tr>
<tr>
<td>Conclusions</td>
<td>ES 5</td>
</tr>
<tr>
<td>Controls and Governance</td>
<td>ES 6</td>
</tr>
<tr>
<td>Compliance with Laws, Regulations and Policies</td>
<td>ES 7</td>
</tr>
<tr>
<td>System Controls</td>
<td>ES 7</td>
</tr>
<tr>
<td>Security Master Data</td>
<td>ES 8</td>
</tr>
<tr>
<td>Reporting</td>
<td>ES 8</td>
</tr>
<tr>
<td>Security Resources</td>
<td>ES 9</td>
</tr>
<tr>
<td>Information Security Risk Management Practices Comparison</td>
<td>ES 10</td>
</tr>
<tr>
<td>Prior Consultant and Audit Recommendations</td>
<td>ES 12</td>
</tr>
<tr>
<td>Operator Access Analyses</td>
<td>ES 12</td>
</tr>
<tr>
<td>General Conclusions</td>
<td>ES 13</td>
</tr>
<tr>
<td>Recommendations</td>
<td>ES 13</td>
</tr>
<tr>
<td>Alamo Colleges Management</td>
<td>ES 13</td>
</tr>
<tr>
<td>SFS District-Northeast Processing Center Management</td>
<td>ES 14</td>
</tr>
<tr>
<td>Information Technology Services Management</td>
<td>ES 14</td>
</tr>
<tr>
<td>Audit Criteria</td>
<td>ES 16</td>
</tr>
<tr>
<td>Audit Information Sources Used</td>
<td>ES 17</td>
</tr>
<tr>
<td>Appendices</td>
<td></td>
</tr>
<tr>
<td>Control Objectives for Information and Related Technology Framework</td>
<td>A</td>
</tr>
<tr>
<td>Enterprise Risk Management - Integrated Framework</td>
<td>B</td>
</tr>
<tr>
<td>FERPA Related Documents</td>
<td></td>
</tr>
<tr>
<td>History of Major Family Educational Rights and Privacy Act Provisions</td>
<td>C.1</td>
</tr>
<tr>
<td>Department of Education – Family Educational Rights and Privacy Act; Final Rules</td>
<td>C.3</td>
</tr>
<tr>
<td>San Antonio College Document Regarding FERPA</td>
<td>C.4</td>
</tr>
<tr>
<td>Texas Administrative Code for Institutions of Higher Education</td>
<td>D</td>
</tr>
<tr>
<td>Alamo Colleges Board Policies</td>
<td></td>
</tr>
<tr>
<td>D.1.1 Compliance with Policies and Procedures</td>
<td>E.1</td>
</tr>
<tr>
<td>F.4.1 Student Records</td>
<td>E.2</td>
</tr>
<tr>
<td>C.2.4 Records Management</td>
<td>E.3</td>
</tr>
<tr>
<td>Description</td>
<td>Page #</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>University of Texas System</td>
<td></td>
</tr>
<tr>
<td>Organization Structure</td>
<td>F.1</td>
</tr>
<tr>
<td>Security Resources</td>
<td>F.2</td>
</tr>
<tr>
<td>The Dallas County Community College District Reporting Structure</td>
<td>G</td>
</tr>
<tr>
<td>The Lone Star College System Reporting Structure</td>
<td>H</td>
</tr>
</tbody>
</table>
OVERVIEW
For 21 years, Alamo Colleges has used an application known as SunGard Student Information System Plus (SIS Plus) to maintain student records. Based on information obtained from the Texas Higher Education Coordinating Board (THECB) Accountability Reports for 2007-2008, the total number of unduplicated students enrolled in Alamo Colleges was 84,623. In fiscal year 2008, transactions processed through the SIS Plus Application for these students resulted in Alamo Colleges reporting revenues of $87.3 million for state appropriations, $52.8 million for tuition and fees, and $85.5 million for grants and contracts/scholarships.

The SIS Plus System processes millions of transactions yearly in various Modules which are divided according to administrative areas. This allows for information to be properly restricted and logically segregated based on functions and job duties. Figure 1 below depicts a high-level summary of these SIS Plus Modules and the number of screens associated with each.

![Figure 1: The SIS Plus Applications](image)

Four Modules support activities related to admissions, student records, billing/receivables, and financial aid management. They also share common data as portrayed by the Module known as Shared Components. This set of screens is composed of information and system functions typically used by more than one administrative area.

Alamo Colleges is responsible for maintaining and protecting the confidentiality, integrity, and security of its student education records. The SIS Plus System allows each institution to implement its own security standards using software known as Series Z Security. This software allows Alamo Colleges to restrict SIS Plus access to specific screens and to specific items of data. The Series Z Security Software also includes reports that can be modified to display summary or detail data that would be helpful to Alamo Colleges Management in monitoring changes to student records or to Operator data.
If access is not managed appropriately or if the application lacks adequate safeguards, then weaknesses in processes and controls will occur which can expose Alamo Colleges to a variety of risks such as:

- Non-compliance with federal and state laws which could result in losing financial aid.
- Theft or modification of information for the purpose of criminal activity such as identity theft, fraud, and E-mail scams which could result in a financial loss.
- Modification of information which could result in Management making decisions with unreliable data.
- Reputational damage and loss of public confidence.

A review of the SIS Plus security processes and controls was approved as part of the Internal Audit Plan for fiscal year 2009. This review was considered critical because Alamo Colleges must comply with federal and state laws such as the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Texas Administrative Code (TAC). In addition, this System stores data and processes millions of transactions which result in substantial Alamo Colleges revenue that is recorded and reported annually.

Under the federal law FERPA, Alamo Colleges has responsibility to protect the privacy of student academic records, including social security numbers (SSN), race, ethnicity, nationality, gender, transcripts and/or grades. This law states that faculty/staff should only access student records for legitimate educational purposes. “The penalty for violating FERPA is the potential loss of federal funding, including grants and financial aid.”

Texas adopted an Administrative Code (TAC) that applies to all state institutions of higher education which addresses establishing security standards based on documented security risk management decisions. TAC states that “measures shall be taken to protect assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information.” The Texas Education Code regards public junior colleges as institutions of higher education.

Alamo Colleges also has approved policies, procedures and regulations related to protecting student records. Policy F.4.1 Student Records and Procedure F.4.1.1 Access to Student Records require that the confidential nature of student records be maintained at all times. These also note that College employees, Trustees, and agents of Alamo Colleges who have a legitimate educational interest in a student’s records should have access to the data. This means that Alamo Colleges Management should establish security controls for access to student data based on a “need to know” basis or only if necessary to perform job duties.
There have been audits of student-related data by the State Auditor’s Office (SAO) and the District’s external auditors. Bi-annually, the SAO selects one of the Alamo Colleges for an audit. They evaluate, on a sampling basis, the accuracy of enrollment for contact hour information reported to the Texas Higher Education Coordinating Board. Annually, the external auditors review student data as part of the financial statement audit. The external auditors also perform Single Audits which evaluate the management and use of federal and state funds. Neither of these external audits has reviewed extensive details in the Series Z Security Software. Student Financial Services (SFS) Management indicated that the Department of Education has never reviewed the financial aid operations and/or the SIS Plus Application; instead they rely on Alamo Colleges Annual Federal and State Single Audits.

SCOPE AND METHODOLOGY
In fiscal year 2009, the Approved Internal Audit Plan included a Student Financial Services Project. Preliminary planning suggested that such a project would require multiple phases due to the five student databases, the millions of records processed by each, and the number of office locations. The project was initially scoped as a performance audit of the department, a computer application and transaction review, a compliance verification, and an award distribution audit.

As a result of the planning and survey activities, it was determined that the computer application and transaction audit should be separated into two phases. This phase focuses on security processes and the controls on January 26, 2009 and July 31, 2009 for the SIS Plus Applications. The evaluation included a review of the Series Z Security Software database which contained information regarding the Operators, access types, and security features.

Further evaluation of the operating environment indicated that there were over three thousand Operators with access, and that the SIS Plus application has over 700 screens available. Approximately sixteen percent of the Operator IDs had inquiry only access. There are no SIS Plus delivered reports showing inquiry attempts. In addition, there were no reports or logs from other Mainframe application management software showing when a User has viewed student data. FERPA requires that there be a record of access to personally identifiable information. Compliance with FERPA could not be completely verified without reports showing operator inquiries.

The Series Z Security Software Reports, including ZBA110 and 115, are not user friendly and have not been maintained using reasonable data standards. Only within the last year has any monitoring occurred by the Information Technology Services (ITS) Department. Data owner monitoring of Operators, by the College Registrars, has been
incomplete and ad hoc. The ITS Department never activated the SIS Plus delivered reporting capability of record changes/updates. The audit team felt that these issues were potential impediments.

The analysis performed for this audit examined in some way all Operators with update access but none with inquiry only. However, no examination of inquiry attempts could be done for these Operators. Additional emphasis was given to Operators associated with the Student Financial Services and the ITS Departments. In addition, a judgmental sample of other Operator IDs was selected for more in-depth analysis.

This report is being issued concurrently with the Student Financial Services Department Operations Review. The phases involving student transactions and employee/dependent financial aid awards are still in-process; these should be completed by year-end.

STATEMENT OF AUDITING STANDARDS
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

ACKNOWLEDGEMENTS
Alamo Colleges Management and Staff were extremely cooperative during this engagement. The Vice Chancellor for Planning, Performance and Information Systems, the District Director of Information Technology Services Department and his staff were helpful in completing this project. The IT Security Officer was instrumental in obtaining timely information. A Client Support Specialist was also supportive in providing information required for this review. Likewise, the Student Financial Services Offices cooperated fully by completing a survey regarding security practices. Campus personnel in the Admissions, Records, and Registrars offices participated by reviewing the conclusions and recommendations, and by attending the formal exit conference.
OBJECTIVES
The objectives established for the SIS Plus security processes and controls project were as follows:

Application Related Controls
- Determine if Alamo Colleges is in compliance with federal and state laws, and Board approved policies and/or Management procedures.
- Determine if the Mainframe security software used by Alamo Colleges has adequate controls to manage the SIS Plus System and if these controls were operating effectively.
- Determine the accuracy and reliability of the security master data, the ZCFILES.
- Determine the availability and usefulness of security related reporting for the SIS Plus System.

Information Security Risk Management
- Determine if resources assigned to manage SIS Plus security are adequate and effective.
- Determine how Alamo Colleges SIS Plus security function compares with other higher education entities.
- Determine if Alamo Colleges Management implemented prior studies/audits recommendations relating to information system security processes and controls.

Access Evaluation
- Determine if the application/security controls for the SFS Offices, the ITS Department and other employees were appropriate, effective and reliable.

CONCLUSIONS
The Series Z Security Software, SIS Plus Application and Alamo Colleges information technology security function are critical components in processing over $225 million of revenue transactions reported annually in the financial statements. Alamo Colleges current processes and controls for these critical components were categorized using the Control Objectives for Information and Related Technology Framework (CobiT) Maturity Model. By using this widely accepted tool, the Board and Management can understand how refined the student financial aid computing technology controls are, or are not. It can also be an indicator as to the reliability of transactions reported in the financial statements. A description of the CobiT maturity categories is included in Appendix A.

Based on interviews with staff, process documentation reviewed, and analysis of security related databases, the existing control environment for these Mainframe applications appears to be in the “repeatable but intuitive” CobiT maturity category. This means that while some controls may be in place they may not be adequately documented and/or are not being verified. It appears that Management has limited preventive and/or detective measures for these computer systems and the related business processes.
It is important that Alamo Colleges improves how it administers and manages the risks related to student information data and security processes. The audit recommendations offered in this report provide ideas to address and/or mitigate these risks. If the recommendations are implemented, Alamo Colleges should move from the current CobiT maturity category to the “defined” level. Most successful organizations, especially those who implement Sarbanes-Oxley requirements, chose to operate within the “defined” level because it demonstrates consistent and repeatable controls based on an appropriate cost-benefit analysis. However, organizations striving for best practices or excellence typically operate at the “managed and measurable” maturity level which requires a greater investment in enterprise risk management.

This audit highlights specific risks including:

- Adoption of a formal internal controls framework, which includes information technology governance standards.
- Compliance with the Family Educational Rights and Privacy Act (FERPA), Texas Administrative Code (TAC), and Alamo Colleges Board policies.
- Effective Series Z Security Software controls, especially passwords and reporting.
- Data standards for entering security master information.
- Comprehensive and formal SIS Plus security procedures/guidelines.
- Reevaluation of ownership and accountability for SIS Plus databases and records.
- Monitoring reports of User activities regarding update or view of student data.
- Sufficiency of resources to support security and compliance activities.
- Job related User access privileges which result in separation of duties issues.

The following summarizes conclusions about how Alamo Colleges Management has addressed these high risk areas:

Controls and Governance
Alamo Colleges has not formally adopted an internal control and information technology governance framework which would incorporate standardized controls for applications like the Series Z Security and SIS Plus Systems. A widely accepted framework used by domestic businesses is the COSO Enterprise Risk Management, as illustrated in Appendix B, which was issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This framework is a well documented common definition of internal controls which has been extensively published for many years. It is a means for Alamo Colleges to train staff, and to evaluate and manage its risk environment. General information technology governance is included in the eight major components of this tool. Many of the conclusions noted in this report would be addressed by Alamo Colleges adopting this or a similarly effective enterprise risk management framework.
Compliance with Laws, Regulations and Policies
Alamo Colleges cannot adequately document its compliance with several federal, state, and local student data requirements related to FERPA – Appendix C, TAC – Appendix D, and Board policies - Appendix E. The consequences of this could be the potential loss of funding, exposure to possible fines or penalties, and erosion of public confidence. These require that Management perform a comprehensive security risk analysis, and implement a formal business continuity and related disaster recovery plan. The current control environment does not appear adequate to safeguard the regulatory designated sensitive student data due in part to using SSNs for student identification, and to not logging or monitoring the use of inquiries. Within the last year, a Student Financial Services’ employee used a Supervisor’s Operator ID to commit a financial aid fraud of about $2,700. During this same period, two faculty members appear to have accessed sensitive student information for non-educational purposes.

System Controls
The Series Z Security Software used in conjunction with the SIS Plus System does not have several commonly used access controls. Industry best practice and the Alamo Colleges ITS Department guidelines recommend that a password should be at least seven characters. The Series Z Security Application has no minimum password length, complexity, expiration, and/or encryption requirements. As a result, over 65 percent of 3,148 Operators had passwords with less than seven characters; in fact, more than 750 Operator passwords have four or less characters. In the San Antonio College (SAC) database, thirty-nine percent of the 890 Operators have not changed their passwords since 2004.

Another common security feature is deactivating a User’s account after three failed log-on attempts within a short time span. Other security enhancements include restricting Operator IDs to specific computers, such as their workstations, and to limit a User’s log-on to a single computer at a time. Alamo Colleges is not using these enhancements for the student related systems, Series Z Security and SIS Plus.

Operators can log-on to an unlimited number of computers simultaneously. Alamo Colleges installs Passport, which is the software necessary to connect to the Mainframe Series Z Security and SIS Plus Systems, on most of the computers in-service, including those in the Welcome Centers at two Colleges. Computers at these locations are logged-on to the Alamo Colleges network each day for student/public use; however, no monitoring of activities occurs at these facilities. There is no time-out feature that breaks the link between Passport, Series Z Security and/or SIS Plus if a computer is inactive for longer than a few minutes while logged-on to the network.
Under current conditions at these locations, former employees can easily continue using Operator IDs that have not been disabled. Generic/Unknown Operator IDs, which have not been disabled, can also be used at these sites by current or former personnel for direct access to SIS Plus. These conditions coupled with weak password features represent major risks and constitute a significant control deficiency.

Security Master Data
There are five distinct Series Z Security Application databases for the SIS Plus System; the master records for Operators do not demonstrate formal data standards. This complicates or prevents meaningful analysis, review, and monitoring of Operators. In many cases, access is not limited to employees’ job duties, and it appears very broad.

As of January 2009, the master data reflects 3,148 Operator IDs for the five databases. The records show that 511 Operator IDs have been disabled or denied by the ITS Department. There are 489 Operator IDs with inquiry only access which includes 125 Generic/Unknown Users with no name or other identifier. Master data for 2,148 Operator IDs with full or partial update access includes 423 Generic/Unknown Users. This group also includes Operator IDs for 121 terminated employees that have not been disabled.

The ITS Department Management provided a one page document of the access set-up guidelines used by the two security personnel; however, the content did not appear sufficiently detailed enough to be effective. Overall, the security master data contains some inaccurate and incomplete information which present other risks for Alamo Colleges and additional significant control deficiencies.

Reporting
The Series Z Security Software includes three system delivered reports for analysis, review, and monitoring purposes. Two reports, ZBA110 and ZBA115, have been set-up by the ITS Department to provide a listing of Operator IDs, their access types, and screens available for inquiry or update. They are not Management friendly, and are too cumbersome to be appropriate analytical tools. In addition, their reliability is questionable based on the master data concerns expressed previously.

The third most critical report known as “On-Line Audit Before/After Change Report” or ZBA120 for system 000 (Security Administration) and 001 (SIS Plus Transactions) has not been implemented for all the Colleges. These reports would allow Management to monitor and review changes made to student related data and to Operator access. At this time, only the version showing Operator changes at San Antonio College has been activated; however, this report has not been scheduled to run daily and/or monthly.
ITS Department Management indicated that the SIS Plus System has been customized over the years. However, the ZBA120 Report version which would have shown transaction changes has not been customized because Management has never requested this report. Internal Audit has been requesting both versions of this report for all Colleges since early 2008 without results.

Security Resources
As mentioned earlier, the SIS Plus and the Series Z Security Software have been used by Alamo Colleges for about 21 years. Security for these Systems has been the responsibility of the ITS Department with Application Programmers or Client Service Support staff performing the daily operational tasks including User access set-up or changes. For some time, the ITS Department has relied on the Admissions and Records Offices at each college to provide limited assistance by reviewing SIS Plus Operator access to supplement their activities. These practices are reminiscent of the traditional approach for handling systems and data security.

In November 2007, the Payroll and Related Business Processes Review audit recommended the establishment of an IT Security Office independent of the IT and Banner Project Departments. This IT Security function was envisioned to be much broader than reviewing security and performing daily operational tasks. The recommendation at that time was for this IT Security Office to report to the Vice Chancellor for Finance & Administration and be responsible for developing information security policies and related regulations/procedures and performing oversight functions. It has become apparent since 2007 that these recommendations would be consistent with the Texas Administrative Code requirements.

The Vice Chancellor for Finance & Administration and the ITS Director at that time partially accepted these recommendations. An IT Security Officer position was created; however, it was assigned to the ITS Department. The job description developed for this position did include responsibilities for developing, implementing and overseeing a District-wide IT security program for Alamo Colleges IT information resources. This job was also expected to consolidate the administration of system access, provide security training, and evaluate processes related to information resources.

The first IT Security Officer was hired in June 2008. This individual's responsibilities include involvement with the SIS Plus, Human Resources and Banner Applications. He was also the backup administrator for the student system databases. In addition, he was engaged with other critical security issues such as the Payment Card Industry (PCI) Data Security Standards and revised federal "Red Flags Rules."
From June 2008 through July 2009, a Client Support Specialist was primarily responsible for administering access/changes for the SIS Plus and the Human Resources Systems. Access requests sent through E-mail or the ITS Department's E-request System were received by this individual who performed the changes without review by or the approval of the IT Security Officer. This person had limited interaction with and did not report to the IT Security Officer.

The IT Security Officer and the Client Support Specialist spent approximately 20 percent of their time specifically on SIS Plus security. The salaries and benefits for the two ITS Department employees was about $126,000. Effectively, Alamo Colleges invested about $25,000 on student data security, or less than .01 percent of the $225 million in revenue accounted for through SIS Plus, in fiscal year 2008.

It does not appear that Alamo Colleges Management has thoroughly evaluated its risks related to student data security, and based its resource allocation decisions for these functions on appropriate cost benefit analyses. It is impractical for one employee to physically set-up system access for thousands of Users, and to perform monitoring duties for six databases, to develop policies, and to document appropriate procedures. Insufficient resource commitments will impact how effectively the District fulfills its administrative capability requirements for the U.S. Department of Education. This resource allocation issue is broader than just the ITS Department staffing since "information security is everyone's business."

**Information Security Risk Management Practice Comparisons**

Information Security has traditionally been the responsibility of IT Departments who manage the Systems. However, increasing regulatory requirements and the inherent risks associated with growing reliance on the use of information technology makes investments in security more crucial. The trend has been for academic institutions to rethink their approach to handling information risk management. A strategic model evolving for organizations of similar size to Alamo Colleges is for the policy, compliance and oversight functions to be segregated from the traditional IT operations areas. This provides a degree of independence and puts the focus on risk management, instead of operations.

This model requires resources in several administrative areas. Typically, IT departments need staff to perform operational tasks such as access change activities based on the instructions/approval of formally designated “data owners.” In addition, institutions need an executive level function to coordinate security efforts across campuses/departments, including information technology, human resources and legal.
The University of Texas System (UT System) has created a security function using the Texas Administrative Code (TAC) as a guideline. They designated a UT System-wide Chief Information Security Officer (CISO) who reports to the System-wide Compliance Officer, see Appendix F. This individual has a staff of three professionals assisting him. In addition, there is an Information Security Officer at each university campus who reports to Executive Management. They also allocate sufficient resources at each institution to fund compliance activities including staffing, training, and monitoring. The Enterprises Systems Group at each college, which is the traditional IT operations area, still performs the routine access changes/updates to the administrative applications.

Dallas County Community College District (DCCCD) initiated its new information security model about two years ago. The Chief Information Privacy and Security Officer (CIPSO), and a professional person, report to the Associate Vice Chancellor for Business Affairs, see Appendix G, while the IT Department reports to the Executive Vice Chancellor for Business Affairs. Besides the District CIPSO Office, there are personnel at the ten campuses who she liaisons with regarding the information risk management functions. In addition, the IT Department has two positions responsible for evaluating processes and systems. Additional personnel in the IT Department perform the hands-on access changes for the major applications, including the Datatel Colleague System. DCCCD uses one student/financial aid database for all of its separately accredited colleges. The CIPSO is using the UT System CISO Office as the model for the DCCCD Office; and is responsible for ensuring District compliance with TAC.

Lone Star College System (LSCS) has implemented the Office of Chief Security Officer (CSO) which reports to the Senior Vice Chancellor/Chief Operating Officer, see Appendix H, while the Office of Technology Services reports to the Vice Chancellor of Information Technology Services. The CSO Office serves as the liaison for the information risk management and security governance program. With a staff of one and a budget of $50,000 for consultants, this office focuses on digital security, information protection and security engineering standards. The Office of Technology Services which is the traditional IT Department performs the hands-on User access changes for the Datatel Colleague System used by all their campuses/locations.

These examples of higher education in Texas illustrate a substantial allocation of resources, primarily personnel, for information risk management functions in order to comply with TAC. All three demonstrate improvements that Alamo Colleges could implement to enhance its compliance with TAC.
Prior Consultant and Audit Recommendations
The Texas Comptroller issued a report in 2003 suggesting that the organization hire a Chief Information Officer and re-evaluate the technology resource allocations between the District and Colleges. Alamo Colleges Management and the Board have benefited from three recent consultant evaluations that touched upon security and the information technology environment. There have also been three external audit Management Letters and Single Audit Reports recommending business continuity and disaster recovery plans, role-based application access, and formalized policies and procedures for data access. At least one prior internal audit documents the need for improved general IT systems controls, especially application access security.

It appears that Alamo Colleges Management is still attempting to address approximately thirty-three recommendations resulting from these detailed evaluations. There is no periodic status report for the Board and Management about these unresolved issues; and no evidence was provided of a formal plan with timelines that addresses the recommendations and/or observations. Delayed or incomplete action on these issues can be seen as a significant deficiency.

Operator Access Analyses
Alamo Colleges has five student databases with more than 2,600 active assigned Operator IDs. As of January 2009, 2,148 of these have update/change and view/inquiry access privileges while 489 have capabilities limited to only view/inquiry. User access to the SIS Plus System is not assigned using a role-based security structure. As a result, there are increased risks for Alamo Colleges and the students because some employees may have more access than is required to carry out their responsibilities. The significance of these risks depends on whether they are mitigated by other controls.

The master data files for the active Operator IDs are massive, complex, and somewhat unreliable. Therefore, several judgmental sample groups were selected for further analysis instead of the entire population. This largest sample group involved 95 current and former Student Financial Services Department (SFS) employees.

The results of analyzing the SFS Operator IDs indicated that six Generic/Unknown User IDs have been used. Five had update and view access while one had been disabled. Alamo Colleges does not know who is using these IDs. There were 15 active Operator IDs with update access assigned to individuals who no longer work at Alamo Colleges. A review of the passwords for each Operator ID showed that 71 were less than seven characters, and 94 had not changed their passwords in a timely manner. Most of the SFS Users had more access than was required to carry out their duties, including multiple databases and screens to the billing, admissions, and student modules.
Typically, Information Technology personnel are not engaged in operating processes and should not require access to production. Twenty-nine Operator IDs associated with the ITS Department had update and/or view access. With access to SIS Plus data, as well as their knowledge of programs, these individuals could potentially make and conceal unauthorized changes to student information.

In addition, the ITS Department has eight Generic/Unknown User IDs with update and/or view access. Four appear to be shared accounts for Help Desk personnel while four are required for SIS Plus functionality. Three Operator IDs with update capability were assigned to individuals who no longer work at Alamo Colleges. A majority of these Operator IDs have password length and change issues. Most of the ITS Department IDs had broad access to screens/data not required to carry-out their job responsibilities.

General Conclusions
These risks may adversely affect the District's/Colleges' ability to initiate, authorize, record, process, and report student revenue data. Opportunities may exist for employees and potentially other individuals to affect transaction processing in ways, including fraud, which might impact revenue reported, and compliance with laws, regulations, and Board policies. There may be more than a remote likelihood that a misstatement of the revenue could occur that would not be detected or identified in a timely manner. Such a misstatement would not need to be financially material. Accounting standards refer to a situation with several significant deficiencies, such as the ones noted in this review, as a material weakness in controls.

RECOMMENDATIONS
Alamo Colleges Management should:
- Propose that the Board of Trustees approve a new policy to adopt and implement a formal internal control framework, preferably the Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM) Framework, see Appendix B.
- Require compliance with the Family Educational Rights and Privacy Act (FERPA).
  - Use an identifying code other than the student SSN.
  - Log all access to the regulatory designated sensitive student data.
- Require compliance with the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, Subchapter C Information Security Standards for Higher Education.
- Require compliance with the Texas Administrative Code, Title 13, Chapter 6, Section 6.10 Texas State Records Retention Schedule regarding retention of security access and reports.
• Establish an Information Security Risk Management Office to report to a Vice Chancellor.
  o Have this Office develop, administer, and monitor a District-wide security program which includes establishing policies, regulations and procedures; conducting employee training; ensuring compliance with legal requirements; and performing a risk assessment of information resources.
  o Ensure that application access standards, which are part of the procedures, are based on role or job responsibilities.
  o Allocate sufficient resources, especially for hiring an Information Security Officer, to manage the program.
• Reevaluate the ownership of student data in SIS Plus and the Banner Modules, and instruct staff on their responsibilities using TAC Rule 202.71 as a guide.
• Implement a continuous communication plan for employees regarding access changes and on-going reviews of security levels to avoid creating negative perceptions.
• Remove the Passport Application from computers located in common areas such as the Welcome Centers and student labs.

SFS District-Northeast Processing Center (District-NEC) Management should:
• Ensure that SFS Department employees have appropriately segregated job responsibilities particularly the SFS District-NEC Programmer and limit their SIS Plus access to assigned duties.

Information Technology Services (ITS) Management should:
• Clarify the IT Security Officers’ role and job duties:
  o Ensure clarification of the interaction with the new Information Security Risk Management Office.
  o Revise the job description to focus more on performing hands-on security reviews and User access set-up for applications.
  o Assign appropriate resources, especially staffing, to support the IT Security Officer in performing daily operational activities.
• Immediately take steps to mitigate the risks identified in this report:
  o Remove access to production data by the ITS Department personnel.
  o Provide ITS staff who require access to SIS Plus, such as the Helpdesk personnel, individual Operator IDs and passwords; changes should be monitored for all ITS Department employees.
  o Assign unique Operator IDs to every SIS Plus User, and disable Generic/Unknown Operator IDs.
  o Prevent the reuse of Operator IDs within a specified time period, usually two fiscal years.
  o Delete access for employees who no longer work for Alamo Colleges.
- Implement the SIS Plus ZBA120 Report known as “On-Line Audit Before/After Change Report” for Systems 000 (Security Administration) and 001 (SIS Plus System) for all college databases and run these reports daily until Banner conversion.

- Develop formal detailed security procedures for administering SIS Plus access, including terminated, retired and transferred employees until an Information Security Risk Management Office is established.

- Disable queries and scripts used by individuals to obtain student information using the Virtual Machine/Conversational Monitor System (VM/CMS) and/or the Terminal Productivity Executive (TPX) Application.
AUDIT CRITERIA
In performing this review the following represent the major criteria used:

  - Family Educational Rights and Privacy Act (FERPA) 34 CFR Part 99
- State Laws website and resources for the:
    - Rule §202.70 – Security Standards Policy
    - Rule §202.71 – Management and Staff Responsibilities
    - Rule §202.72 – Managing Security Risks
    - Rule §202.74 – Business Continuity Planning
    - Rule §202.75 – Information Resources Security Safeguards
- Alamo Colleges Board Policies and Procedures (http://www.alamo.edu/district/ethics/policies.htm)
  - DH (Local) Employee Standards of Conduct dated 10/7/2008
  - F.4.1 (Policy) Student Records dated 5/19/2009
  - FJ (Local) Student Records dated 2/26/2007
  - C.2.4 (Policy) Records Management dated 8/18/2009
  - CIA (Local) Equipment, Supplies, and Office Management: Records Management Program
    - Records Retention Schedule (Abbreviated) dated 8/22/2008
- Alamo Colleges Ethics Handbook dated 1/2009 (http://www.alamo.edu/district/ethics/)
- Alamo Colleges Acceptable Computer Use dated 7/13/2004
- Alamo Colleges Employees Services Department’s website
  - Job Descriptions (http://www.alamo.edu/ACCD/hr/JO/ALLJOBS.htm)
- Employee Handbook, 7/27/2005 (http://www.alamo.edu/accd/hr/handbook.htm)
- ITS Department Security Awareness and Education Training Guide version 1.1
- Control Objectives for Information and related Technology (CobiT) Control Framework version 4.1

ES Page 16 of 17
AUDIT INFORMATION SOURCES USED
For this review, the following are the major sources of information and data used:

- Alamo Colleges Digital Documents System (Webxtender) - Folder PAR
- Human Resources System records
  - 011 Empl/Appd Add/Maintain
  - 012 Corporation Root Add/Main
  - L16 Assignments List
- Series Z Security Reports
  - ZBA115 – Screen Access Verification as of 1/26/2009 and 7/31/2009
  - ZBA120 – Online Audit Before/After Change Report (not set-up)
- SunGard SCT Documentation
  - SCT Plus Student Information System Shared Components User Guide
    version 1.20 dated 12/2004
- Series Z Security Files (ZCFIIE) for all five colleges as of 1/26/2009
- Prior Audit/Consultant Reports
  - Information Security Assessment by the Denim Group dated 12/2008
  - Information Technology Assessment by Kaludis Consulting dated 12/2007
  - Information Technology Review Spring 2006
- Information Security Risk Management Practice Comparison Sources
  - The University of Texas System, www.utsystem.edu
  - Dallas County Community College District, www.dcccd.edu
  - Lone Star College System, www.lonestar.edu
CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (CobiT) FRAMEWORK

In 1996, the Information Systems Audit and Control Association and the Information Technology Governance Institute developed a tool to assist organizations understand their information technology (IT) processes and the level of security and controls necessary to protect their assets. This governance model, called the CobiT Framework, focuses specially on IT controls, while another model, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework focuses on financial operations. Both provide guidance on evaluating controls and provide a set of categories to measure the status of an organization’s internal control environment. The difference is that COSO is useful for all levels of Management, while CobiT is useful for IT Management.

<table>
<thead>
<tr>
<th>CobiT Maturity Model for Internal Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Level</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>0 Non-existent</td>
</tr>
<tr>
<td>1 Initial/Ad Hoc</td>
</tr>
<tr>
<td>2 Repeatable but Intuitive</td>
</tr>
<tr>
<td>3 Defined</td>
</tr>
<tr>
<td>4 Managed and Measurable</td>
</tr>
<tr>
<td>5 Optimized</td>
</tr>
</tbody>
</table>

Source: The IT Governance Institute, CobiT 4.1 dated 2007

Appendix A
1 of 1
ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK

The COSO ERM Framework defines the essential components of and guidance for enterprise risk management. It consists of eight interrelated components to help organizations manage their risks. By applying it, organizations can operate more effectively and efficiently, maintain the integrity of their financial reports, and ensure compliance with applicable laws and regulations. The COSO ERM tool should provide Alamo Colleges with the basis for improved risk-informed decision-making.

Committee of Sponsoring Organizations
Enterprise Risk Management (COSO ERM) Framework

Internal Environment:
Encompasses the tone of the organization, influencing the risk consciousness of its people and is the basis for all other components of ERM, providing discipline and structure.

Objective Setting:
Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives.

Risk Assessment:
Allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives – likelihood and impact.

Event Identification:
Management identifies potential events that can affect the entity and determines whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives.

Risk Response:
Management determines how it will respond to the assessed relevant risks. Responses fall into the following categories:
Avoidance, Reduction, Sharing or Acceptance

Control Activities:
Policies and procedures that help ensure that management's risk responses are carried out. These occur throughout the organization at all levels and in all functions.

Information and Communication:
Pertinent information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs, flowing down, across, and up the organization.

Monitoring:
ERM is monitored – assessing the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

FERPA is a federal law that protects the privacy of student educational records which became effective on November 1974. The law has been amended by Congress several times. The history of major FERPA provisions was obtained from the website at http://www.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html.

---

**Legislative History of Major FERPA Provisions**

The Family Educational Rights and Privacy Act of 1974 ("FERPA"), § 513 of P.L. 93-380 (The Education Amendments of 1974), was signed into law by President Ford on August 21, 1974, with an effective date of November 19, 1974. FERPA was enacted as a new § 438 of the General Education Provisions Act (GEPA) called "Protection of the Rights and Privacy of Parents and Students," and codified at 20 U.S.C. § 1232g. It was also commonly referred to as the "Buckley Amendment" after its principal sponsor, Senator James Buckley of New York. FERPA was offered as an amendment on the Senate floor and was not the subject of Committee consideration. Accordingly, traditional legislative history for FERPA as first enacted is unavailable.

Senators Buckley and Pell sponsored major FERPA amendments that were enacted on December 31, 1974, just four months later, and made retroactive to its effective date of November 19, 1974. These amendments were intended to address a number of ambiguities and concerns identified by the educational community, including parents, students, and institutions. On December 13, 1974, these sponsors introduced the major source of legislative history for the amendment, which is known as the "Joint Statement in Explanation of Buckley/Pell Amendment" ("Joint Statement"). See Volume 120 of the Congressional Record, pages 39862-39866.

Congress has amended FERPA a total of nine times in the nearly 28 years since its enactment, as follows:

- P.L. 93-568, Dec. 31, 1974, effective Nov. 19, 1974 (Buckley/Pell Amendment)
- P.L. 96-46, Aug. 6, 1979 (Amendments to Education Amendments of 1978)
- P.L. 96-88, Oct. 17, 1979 (Establishment of Department of Education)
- P.L. 101-542, Nov. 8, 1990 (Campus Security Act)
- P.L. 103-382, Oct. 20, 1994 (Improving America's Schools Act)
- P.L. 106-386, Oct. 28, 2000 (Campus Sex Crime Prevention Act)

---

1 The Improving America's Schools Act (1994) renumbered GEPA so that FERPA is now § 444.

2 Congress addressed two additional and related privacy concerns in P.L. 93-380 -- Protection of Pupil Rights, enacted as § 439 of GEPA (now §445) and codified at 20 U.S.C. § 1232h, and Limitation on Withholding of Federal Assistance, enacted as § 440 of GEPA (now §446) and codified at 20 U.S.C. § 1232i.
Alamo Colleges  
Student Information System Plus Security Processes and Controls Review-Executive Summary  
July 31, 2009

**Code of Federal Regulations - Title 34 - Education - Part 99 - Family Educational Rights and Privacy Act (FERPA) of 1974**

The FERPA law applies to all institutions that receive funds under any program administered by the U.S. Department of Education. Excerpts from FERPA regarding applicability, purpose, and several definitions are shown below. These were obtained from the FERPA website at [http://www.ed.gov/policy/gen/reg/ferpa/index.html](http://www.ed.gov/policy/gen/reg/ferpa/index.html).

### PART 99—FAMILY EDUCATIONAL RIGHTS AND PRIVACY

#### Subpart A—General

§ 99.1 To which educational agencies or institutions do these regulations apply?

- Except as otherwise noted in § 99.10, this part applies to an educational agency or institution to which funds have been made available under any program administered by the Secretary, if—
  1. The educational institution provides educational services or instruction, or both, to students; or
  2. The educational agency is authorized to direct and control public elementary or secondary, or postsecondary educational institutions.
- This part does not apply to an educational agency or institution solely because students attending that agency or institution receive non-monetary benefits under a program referenced in paragraph (a) of this section, if no funds under that program are made available to the agency or institution.
- The Secretary considers funds to be made available to an educational agency or institution of funds under one or more of the programs referenced in paragraph (a) of this section—
  1. Provided to the agency or institution by grant, cooperative agreement, contract, subgrant, or subcontract; or
  2. Provided to students attending the agency or institution and the funds may be paid to the agency or institution by those students for educational purposes, such as under the Pell Grant Program and the Guaranteed Student Loan Program (titles IV A-1 and IV-B, respectively, of the Higher Education Act of 1965, as amended).
- If an educational agency or institution receives funds under one or more of the programs covered by this section, the regulations in this part apply to the recipient as a whole, including each of its components (such as a department within a university).

(Authority: 20 U.S.C. 1232g)

§ 99.2 What is the purpose of these regulations?

The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.

(Authority: 20 U.S.C. 1232g)

§ 99.3 What definitions apply to these regulations?

The following definitions apply to this part:


(Authority: 20 U.S.C. 1232g)

- **Disclosure** means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any other party, by any means, including oral, written, or electronic means.

(Authority: 20 U.S.C. 1232g(b)(1))

- **Educational agency or institution** means any public or private agency or institution to which this part applies under § 99.1(a).

(Authority: 20 U.S.C. 1232g(a)(3))

- **Education records** means any public that are: (1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

- **Personally identifiable information** includes, but is not limited to:
  1. The student’s name;
  2. The name of the student’s parent or other family member;
  3. The address of the student or student’s family;
  4. A personal identifier, such as the student’s social security number or student number;
  5. A list of personal characteristics that would make the student’s identity easily traceable; or
  6. Other information that would make the student’s identity easily traceable.

(Authority: 20 U.S.C. 1232g)

- **Record** means any information recorded in any way, including but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

(Authority: 20 U.S.C. 1232g)
Department of Education (DOE) - Family Educational Rights and Privacy Act (FERPA); Final Rules

The DOE created a document regarding interpretations of FERPA to implement provisions of the USA Patriot Act and the Campus Sex Crimes Prevent Act which added disclosure exceptions. Below is an excerpt indicating that personally identifiable information includes a student’s name and Social Security Number. Other information such as address, birth place, race, ethnicity, gender can also indirectly identify a student. The ITS Department contains a link to this policy guidance document which is located at the website http://www.ed.gov/policy/gen/uid/fpco/ferpa/index.html.

FR Doc E8-28864[Federal Register: December 9, 2008 (Volume 73, Number 237)]
[Rules and Regulations]
[Page 74805-74855]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr09de08-8]
Personally Identifiable Information and De-Identified Records and Information (Sec. Sec. 99.3 and 99.31(b))

Family Educational Rights and Privacy; Final Rule

DEPARTMENT OF EDUCATION

34 CFR Part 99

RIN 1855-AA05
[Docket ID ED-2008-OPEPD-0002]

AGENCY: Office of Planning, Evaluation, and Policy Development, Department of Education.

ACTION: Final regulations.

SUMMARY: The Secretary amends our regulations implementing the Family Educational Rights and Privacy Act (FERPA), which is section 444 of the General Education Provisions Act. These amendments are needed to implement a provision of the USA Patriot Act and the Campus Sex Crimes Prevention Act, which added new exceptions permitting the disclosure of personally identifiable information from education records without consent. The amendments also implement two U.S. Supreme Court decisions interpreting FERPA, and make necessary changes identified as a result of the Department's experience administering FERPA and the current regulations.

(a) Definition of Personally Identifiable Information

...The simple removal of nominal or direct identifiers, such as name and SSN (or other ID number), does not necessarily avoid the release of personally identifiable information. Other information, such as address, date and place of birth, race, ethnicity, gender, physical description, disability, activities and accomplishments, disciplinary actions, and so forth, can indirectly identify someone depending on the combination of factors and level of detail released.
San Antonio College Document Regarding FERPA
Below is an example of communication about the FERPA regulation from the San Antonio College (SAC) Admission and Records website (http://www.alamo.edu/sac/admrec/FERPA.htm).

| FERPA |
| FACULTY, STAFF AND ADMINISTRATORS |

WHAT IS FERPA?
FERPA stands for Family Educational Rights and Privacy Act of 1974, as Amended. It is commonly known as FERPA, the Privacy Act or the Buckley Amendment. It is a federal law designed to protect the privacy of educational records, to establish the right of students to inspect and review their educational records and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings.

FERPA allows release of specified items but does not require it. Items that may be released are called directory information. San Antonio College has classified these items as directory information: student's name, dates of attendance, major, classification, enrollment status (full-time or part-time), previous institution(s) attended, degree(s) awarded, academic honors/awards.

Students may place a directory hold on any or all of this information by completing the Withholding Directory Information form and turning it in to the Admissions and Records Office in room 216 Fletcher Administration Center. It is available on the Admissions and Records web page or in room 216 Fletcher Administration Center. After this information is entered, a statement will appear on the monitor screen that the student has blocked his/her information. Check screen 011 for directory items that have been restricted and may not be released without a signed statement from the student.

Items that can never be identified as directory information are a student's social security number or institutional identification number, address, telephone number, date of birth, race/ethnicity, citizenship, nationality, gender, grades, grade point average or class schedule.

WHAT IS A STUDENT EDUCATIONAL RECORD?
A student educational record is any record with certain exceptions, maintained by an institution that is directly related to a student or students. This record can contain a student's name, or students' name, or information from which an individual student, can be personally (individually) identified. These records include files, documents and materials in whatever medium (handwriting, print, monitor screen, tapes, disks, film, microfilm, microfiche or notes) that contain information directly related to students and from which students can be personally identified.

If ever in doubt whether information may be released, DON'T. Please call one of the directors in Admissions and Records. They will help you determine if the information is an educational record and/or whether it may be disclosed without written consent. To be safe, always think written consent.

WHAT IS LEGITIMATE EDUCATIONAL INTEREST?
A legitimate educational interest shall mean any authorized interest, or activity undertaken in the name of the college for which access to an educational record is necessary or appropriate to the proper performance of the undertaking.

This means if a student is assigned to you for advising, you have a legitimate educational interest and may access his/her records. If a good friend asks you to tell him the grades his daughter has made, DON'T. This has two problems. First unless this student is your advisee, you do not have a legitimate educational interest. Second if the parent has not filed the Certification of Dependency form with the Admissions and Records Office, the parent is not entitled to this information.
POSTING OF GRADES BY FACULTY
The public posting of grades either by the student’s name, institutional student identification number, social security number or any portion of the number without the student’s written permission is a violation of FERPA. This includes posting grades to a class/institutional website and applies to any public posting of grades for students taking distance education courses. Even with names obscured, numeric student identifiers are considered personally identifiable information. The practice of posting grades by social security number, student identification number or any portion of the number violates FERPA. Notification of grades via a postcard violates a student’s privacy.

There is no guarantee of confidentiality of sending grades via the Internet outside of the ACCD System. The institution would be held responsible if an unauthorized third party gained access, in any manner, to a student's education record through any electronic transmission method. A third party in this definition could be parents or guardians, boyfriend or girlfriend, roommate, etc. Only secure web sites are approved by FERPA for accessing grade information.

PENALTIES FOR VIOLATING FERPA
The Family Policy Compliance Office reviews and investigates complaints of violations of FERPA. The penalty for violating FERPA is loss of all federal funding, including grants and financial aid.

SPECIAL “DON’TS” FOR FACULTY
To avoid violations of FERPA rules, DO NOT:

- At any time use the social security number, institutional identification number or any portion of the number of a student in a public posting of grades
- Ever link the name of a student with that student's social security number, institutional identification number in any public manner
- Leave graded tests or papers in a stack for students to pick up by sorting through the tests or papers of all students
- Circulate a printed class list with student name and social security number/institutional identification number or grades as an attendance roster.
- Discuss the progress of any student with anyone other than the student (including parents/guardians) without the consent of the student
- Provide anyone with lists of students enrolled in your classes for any commercial purpose
- Provide anyone with student schedules or assist anyone other than college employees in finding a student on campus

QUESTION AND ANSWER SESSION
The Director of Admissions and Records (210-733-2589) is available to participate in a FERPA question and answer session for any department or college faculty meeting.

Please refer any parent/guardian seeking information on student covered by FERPA, to the Admissions and Records Office (210) 733-2583.
Texas Administrative Code (TAC) for Institutions of Higher Education

This is a listing of the Texas Administrative Code related to Institutions of Higher Education evaluated during this audit. Rules §202.73 Managing Physical Security, §202.76 Security Incident, and §202.78 Removal of Data from Data Processing Equipment were not part of the scope of this audit as depicted with an “×”.

---

**Texas Administrative Code**

**TITLE 1**

ADMINISTRATION

**PART 10**

DEPARTMENT OF INFORMATION RESOURCES

**CHAPTER 202**

INFORMATION SECURITY STANDARDS

**SUBCHAPTER C**

SECURITY STANDARDS FOR INSTITUTIONS OF HIGHER EDUCATION

Rules

- §202.70 Security Standards Policy ✓
- §202.71 Management and Staff Responsibilities ✓
- §202.72 Managing Security Risks ✓
- §202.73 Managing Physical Security ×
- §202.74 Business Continuity Planning ✓
- §202.75 Information Resources Security Safeguards ✓
- §202.76 Security Incidents ×
- §202.77 User Security Practices ✓
- §202.78 Removal of Data from Data Processing Equipment ×
Alamo Colleges
Student Information System Plus Security Processes and Controls Review - Executive Summary
July 31, 2009

Alamo Colleges Board Policies – D.1.1 Compliance with Policies and Procedures
There were three specific Board policies used as criteria for this audit. The policies involved compliance, student records and records management. All three policies have been in existence for several years but the format and numbering scheme changed in year 2009.

D.1.1 (Policy) Compliance with Policies and Procedures
Responsible Department: Employee Services
Board Adoption: 4-28-09
Last Board Action: 4-28-09

The College District and all its employees shall abide by:

1. The College District policies and procedures in this manual;
2. The College District Code of Conduct;
3. All applicable laws; and
4. Any other policies, procedures, practices, and guidelines that impose duties, requirements, or standards attendant to their status as College District employees to the extent that they do not conflict with College District policies and procedures in this manual or applicable laws.

Noncompliance may result in disciplinary action, up to and including termination of employment. The College District policies and procedures contained in this manual supersede all previous versions and all other procedures, practices, and guidelines.

To the extent that any practices, procedures, handbooks, or similar statements of rules or policies conflict with the policies and procedures in this manual, the policies and procedures in this manual shall control. To the extent that any policy or procedure in this manual is inconsistent with applicable law, the applicable law shall control.
Alamo Colleges Board Policies – F.4.1 Student Records

F.4.1 (Policy) Student Records
Responsible Department: Vice Chancellor for Student Success,
Vice Chancellor for Academic Success

Board Adoption: 5-19-09; Last Board Action: 5-19-09

Each college President shall develop and maintain a comprehensive system of student records and reports dealing with all facets of that college’s program operation under the direction of the Vice Chancellor for Student Success and the College District records manager. These data and records shall be stored in a safe and secure manner and shall be conveniently retrievable for utilization by authorized school personnel.

Confidentiality
The confidential nature of the student’s records shall be maintained at all times.

Custodians of Records
The registrar or designee at each college is custodian of all records for currently enrolled students and for all official academic records. The address of the registrar for each college shall be maintained on the college’s website and included in the college catalog.

Types of Records
Education records may include, but are not limited to:
1. Admissions data, personal and family data.
2. Class schedules
3. Standardized test data, including scholastic, aptitude, and interest ratings.
4. Achievement records, as determined by tests, recorded grades, and teacher evaluation.
5. Attendance record.
6. Records of faculty, counselors, or administrative conferences with the student or pertaining to the student.
7. Disciplinary records.
8. Copies of correspondence with parents and others concerned with the student.
9. Records transferred from secondary schools and other post-secondary institutions in which the student has been enrolled.
10. Records pertaining to participation in student activities including awards or recognition by the colleges.
11. Information relating to student participation in special programs.
12. Records of tuition and fees paid and outstanding.
13. Other records that may contribute to understanding of the student.
15. Records of scholastic disciplinary actions.
17. Scholarships or other financial awards.
18. Academic awards or recognition by the colleges.
Procedure F.4.1.1 Access to Student Records
Procedure F.4.1.2 Amendments to Student Records

FJ(Legal) – Student Records
FJ(EXHIBIT) – Students Records
C.2.4 (Policy) Records Management
Responsible Department: Legal Services, Vice Chancellor for Finance and Administration
Board Adoption: 8-18-09
Last Board Action: 8-18-09

Records Management Program
The College District shall provide for efficient, economical, and effective controls over the creation, distribution, organization, maintenance, use, and disposition of all Records Management Program records through a comprehensive system of integrated procedures for the management of records from their creation to their ultimate disposition, consistent with requirements of the Texas Local Government Records Act.

Records Management Officer
The Chancellor or designee shall serve as Records Management Officer for the College District. The Chancellor may delegate this authority to an individual in each college of the College District. In the event of the resignation, retirement, dismissal, or removal of the Chancellor’s designee, the Chancellor shall promptly designate a replacement. The individual designated as Records Management Officer shall file his/her name with the director and librarian of the Texas State Library within thirty days of the date of designation, as provided by state law.

Procedure C.2.4.1 Records Management
CIA(LEGAL) - Equipment, Supplies, and Office Management: Records Management Program
Alamo Colleges
Student Information System Plus Security Processes and Controls Review - Executive Summary
July 31, 2009

The University of Texas System (UT System) Organization Structure
The organization chart for the UT System was obtained from the website at http://www.utsystem.edu/cha/files/UTSystemOrgChart.pdf. This was used in comparing Alamo Colleges reporting structure to other higher education institutions. The Chief Information Security Officer reports to the System-wide Compliance Officer, who reports to the Chancellor.
The University of Texas System (UT System) Security Resources

The list of UT System Information Security staff was obtained from the website at http://www.utsystem.edu/ciso/Staff/StaffListing.htm. This was used in comparing Alamo Colleges resources to other higher education institutions. This does not include the security staff resources at each of the nine academic and four health institutions.
The Dallas County Community College District (DCCCD) Reporting Structure
The reporting structure for DCCCD was obtained from the Chief Information Privacy & Security Officer (CIPSO). It was used in comparing Alamo Colleges reporting structure to other higher education institutions. The CIPSO reports to the Associate Vice Chancellor of Business Affairs.
The Lone Star College System (LSCS) Reporting Structure
The reporting structure for LSCS was obtained from the Office of Chief Security Officer (CSO). It was used in comparing Alamo Colleges reporting structure to other higher education institutions. The CSO reports to the Senior Vice Chancellor/Chief Operating Officer.