6107.1 Under the provisions of Public Law 93-380, a student attending a college has the right to inspect "any and all" official files that relate directly to that student. It is the policy of the college not to release information about present or former students to anyone except as noted below:

A. When the student provides a written request for a record release.
B. When requested by representatives of state or federal educational agencies.
C. When the information is requested pursuant to a subpoena or court order.

6107.2 Records may not be released to relatives or friends unless the student gives written permission.

6107.3 Requests for exceptions or unusual requests shall be directed to the Vice President of Instruction/ Student Services.

6107.4 Requests from law enforcement officials shall be directed to the Vice President of Instruction/Student Services.

6107.5 INFORMATION SECURITY PROGRAM

Overview: This summarizes Big Bend Community College's (the Institution's) comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm. The Program incorporates the Institution's policies and procedures and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation Representatives: The Institution's Director of Financial Aid and the Controller are designated as the Program Officers who shall be responsible for coordinating and overseeing the Program. The Program Officers may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officers or their designees.

Scope of Program: The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

1. Risk Identification and Assessment. The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuses, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officers will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- *Employment training and management.* The Program Officers will coordinate with representatives in the Institution's Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area.

- *Information Systems and Information Processing and Disposal.* The Program Officers will coordinate with representatives of the Institution's Information Systems department to assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current policies and procedures relating to Acceptable Use of the Institution's network and network security, document retention and destruction. The Program Officers will also coordinate with the Institution's Information Systems department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks.* The Program Officers will coordinate with the Institution's Information Systems department to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officers may elect to delegate to a representative of the Information Systems department the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officers will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalating procedures.

3. Overseeing Service Providers. The Program Officers shall coordinate with those responsible for the third party service procurement activities among the Information Systems department and other affected departments to raise awareness of, and to institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officers will work with the Center for Information Services and the Office of the Attorney General to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Office of the Attorney General. These standards shall apply to all existing and future contracts entered into with such third party service providers, provided that amendments to contracts entered into prior to June 24, 2002 are not required to be effective until May 2004.

4. Adjustments to Program. The Program Officers are responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program. A security audit of the BBCC Information Systems will be conducted by the Department of Information Services in conjunction with the Auditors Office by October 3, 2003. The purpose of the aforementioned audit is to review BBCC security measures, identify security weaknesses and recommend security changes that will provide a comprehensive approach to adjusting existing programs.