INFORMATION SECURITY

INFORMATION SECURITY PROGRAM

The College President shall approve an information security program designed to address the security of the College District's information resources against unauthorized or accidental modification, destruction, or disclosure. This program shall include procedures for risk assessment and for information security awareness education for employees when hired and ongoing program for all users, as well as compliance with all applicable laws.

The College President or designee shall designate an information security officer (ISO) who is authorized to administer the information security requirements under the law. The College President or designee shall notify the Texas Department of Information Resources (DIR) of the individual designated to serve as the ISO.

The College shall adopt procedures for addressing the privacy and security of information resources, including the College's website and mobile applications and shall submit, as required, the procedures to DIR for review.

The procedures must require the developer of a website or application for the College District that processes confidential information to submit information regarding the preservation of the confidentiality of the information. The College must subject the website or application to vulnerability and penetration test before deployment.

The College shall submit a biennial information security plan to DIR in accordance with law.

The ISO shall report annually to the President on the effectiveness of the College's information security policies, procedures, and practices in accordance with law and administrative procedures.

SECURITY BREACH NOTIFICATION

Upon discovering or receiving notification of a breach of system security or a security incident, as defined by law, the College District shall disclose the breach or incident to affected persons or entities in accordance with the time frames established by law. The College shall also assess the significance of a security incident and report urgent incidents to DIR and law enforcement in accordance with law and, if applicable, DIR requirements.

The College District shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the College District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the College District's Web site.

4. Publication through broadcast media.

The College District must provide summary reports of security incidents in accordance with DIR guidelines.

The College District shall include in any vendor or third-party contract the requirement that the vendor or third party report information security incidents to the College District in accordance with current law and administrative procedures.

ACCESS BY INDIVIDUALS WITH DISABILITIES

The College President or designee shall develop procedures to ensure that individuals with disabilities have access to the College District's electronic and information resources similar to individuals without disabilities. The procedures shall include the standards and specifications in accordance with 1 Administrative Code Chapter 213.

SECURITY AND PRIVACY

The security and integrity of the College District's electronic and technology resources are essential. Therefore, priority shall be given to maintaining system security and integrity, backing up the system, and general maintenance of the system. The following relate to system security, integrity, and privacy:

1. The College President shall appoint an administrator responsible for developing and maintaining College District procedures regarding security and privacy of computer data, software, and hardware.

2. Any student or employee use of College District electronic and technology resources is a privilege that may be revoked for violation of this policy, regardless of the need for such use in performing assigned duties.

3. A student or employee (regardless of employment contract or tenure status) found to be involved in infractions of this policy or civil or criminal laws regarding College District electronic and technology resources security and privacy shall be subject to disciplinary actions including, but not limited to, revocation of user privileges, suspension, dismissal, prosecution, and restitution for damages. Involvement, as used here, includes, but is not limited to, participating, encouraging, aiding, or failing to report known infractions.

4. Under the authority of the College President, the department of information technology shall have the authority to monitor all electronic and technology resources to protect the integrity of the College District's systems, computing software, workstations, and lab facilities. Designated personnel from the IT department shall have the authority to access files when necessary for the maintenance of the electronic and technology

systems. When performing maintenance, every effort shall be made to ensure the privacy of a user's files. However, if violations are discovered, the violation(s) shall be reported immediately to the director of human resources, the appropriate vice president, and the College President.

5. Some jobs or activities of the College District involve access to resources critical to electronic and technology resources security and privacy. The College District may require employees or students involved in these jobs or activities to disclose personal histories, participate in special training, or sign special agreements concerning computer use.

6. All students and employees shall cooperate with official state and federal law enforcement authorities in aiding the investigation and prosecution of any suspected infraction of security and privacy involving either College District personnel or College District electronic and technology resources.

7. The College District shall make every effort to ensure the integrity of its various systems. All electronic and technology resources available to users offer some form of dataset protection, which can be modified by an authorized user as needed. However, none of the systems offer absolute security. Therefore, users shall not place sensitive information on a publicly accessible system.

8. The College District shall not be responsible for the safe storage of student-generated files. Each student shall be responsible for maintaining copies of any information and work created on College District equipment. The College District shall not be responsible for any loss of student information or student-generated files from College District electronic and technology resources equipment, regardless of the cause.

IDENTITY THEFT PREVENTION

The College President or designee shall approve and maintain an Identity Theft Prevention Program designed to prevent the unauthorized distribution or theft of personal/confidential information pursuant to the Federal Trade Commission's Red Flags Rule (Rule), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. [16 CFR 681.2]

SECURITY AND PRIVACY

The College District has identified the following areas requiring oversight for the prevention of identity theft:

1. Customer/consumer information submitted to and required by the College District or by a third party;

2. Employee information submitted to and required by the College District or by a third party; and

3. Confidential information of an employee or a student provided to a third party.

OBJECTIVES

The objectives of the Identity Theft Prevention Program shall be:

1. To ensure the security and confidentiality of customer/consumer information;
2. To prevent disclosure of an employee's personal/confidential information;
3. To protect and secure personal/confidential information stored in departmental file cabinets;
4. To protect and secure personal/confidential information stored in the College District's ERP system or other computers owned by the College District;
5. To protect and secure personal/confidential information provided to third parties;
6. To protect against any anticipated threats or hazards to the security or integrity of such information; and
7. To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any employee or student/customer/consumer.