Orientation

The Board and the District President will provide an orientation for new Board members within the calendar year of their election to assist them in understanding the Board's function, policies, and procedures. Assistance given in the orientation of new Board members may include the following, as appropriate or available:

1. Selected materials on the responsibilities of being a contributing member of the Board.
2. Material pertinent to meetings and an explanation of its use.
3. Invitations to meet with the District President and other administrative personnel designated by the District President to discuss services the administration performs for the Board.
4. Access to a copy of the Board's policies and administrative regulations and other documents and information currently in use by other Board members.
5. Information regarding appropriate meetings and workshops.
6. A formal orientation on legal and budgetary oversight responsibilities of the Board.
7. Other information and activities as the Board or the District President deems useful in fulfilling the role of Board member.

The District President will work with the Board to address the training needs of Trustees.

Cybersecurity Training

The ~~District President~~District President or designee will determine, from the list of cybersecurity training programs certified by the Department of Information Resources (DIR) and published to DIR's website, the cybersecurity training program to be used in the College District. ~~The District President~~The District President in consultation with the Board Chair may remove access to the College District's computer systems and databases for noncompliance with training requirements as appropriate.

The ~~District President~~District President will periodically require an internal review of the College District to ensure compliance with the cybersecurity training requirements.

Public Information ~~Coordinator~~Act Training

The Chief Public Relations Officer or designee will fulfill the responsibilities of the public information coordinator and will receive, on behalf of Board members, the Public Information Act (PIA) training specified by Government Code 552.012 to be completed no later than the 90th day after the member takes the oath of office.

After Election or Appointment

After a Violation

A Board member who receives written notice from the Attorney General that the member must complete the PIA training described

by Section 552.012 following the College District's failure to comply with a PIA requirement shall complete the training within the time-lines described in law.

~~The District President~~The District President is responsible for the security of the College District's information resources. ~~The District President~~The District President or designee will develop procedures for ensuring the College District's compliance with applicable law.

Information Security Officer

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

Information Security Program

The District President or designee will annually review and approve an information security program designed in accordance with law by the ISO to address the security of the information and information resources owned, leased, or under the custodianship of the College District against unauthorized or accidental modification, destruction, or disclosure. The program will include procedures for risk assessment and for information security awareness education for employees when hired and an ongoing program for all users.

The information security program must be submitted biennially for review by an individual designated by the ~~District President~~District President and who is independent of the program to determine if the program complies with the mandatory security controls defined by DIR and any controls developed by the College District in accordance with law.

College District Website and Mobile Application Security

~~The District President~~The District President or designee will adopt procedures addressing the privacy and security of the College District's website and mobile applications and submit 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 District must subject the website or application to a vulnerability and penetration test before deployment.

Covered Social Media Applications

The District President or designee shall adopt procedures prohibiting the installation or use of a covered social media application, as defined by law, on a device owned or leased by the College District and requiring the removal of any covered applications from the device.

Exception

The procedures shall permit the installation and use of a covered application for purposes of law enforcement and the development

and implementation of information security measures. The procedures must address risk mitigation measures during the permitted use of the covered application and the documentation of those measures.

Reports

Information Security Plan

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

Effectiveness of Policies and Procedures

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

Security Incidents

By the College District

The College District will 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.

Generally

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 ~~will~~shall disclose the breach or incident to affected persons or entities in accordance with the time frames established by law.

The College District will 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 website.
4. Publication through broadcast media.

The College District may also work with the United States Computer Emergency Readiness Teams (US-CERT), Information Sharing and Analysis Center (ISAC), or other trusted third-party broker to help research and resolve the issue.

By Vendors and Third Parties

The College District will 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 law and administrative procedures.

Monthly Reports

The College District must provide summary reports of security incidents monthly to DIR in accordance with the deadlines, form, and manner specified by law and DIR.

Student Code of Conduct

College District students are both citizens and members of the academic community. As citizens and students, they enjoy the same freedom of speech, peaceful assembly, and right of petition that other citizens enjoy. As members of the academic community, they are subject to the obligations that are theirs by virtue of this membership.

The College District expects its students to conduct themselves in a manner that reflects credit upon the institution they represent. There are two basic standards of behavior required of all students:

1. They will adhere to College District policies and municipal, county, state, and federal laws; and
2. They will not interfere with or disrupt the orderly educational processes of the College District.

Students are entitled to only those immunities or privileges by law as enjoyed by other citizens. In the event any provision of this policy conflicts with the laws of the State of Texas or the United States of America, the state or federal law will prevail.

Scholastic Dishonesty

Every member of the College District community is expected to maintain the highest standards of academic integrity. All work submitted for credit is expected to be the student's own work. The College District may initiate disciplinary proceedings against a student or program applicant accused of scholastic dishonesty. While specific examples are listed below, this is not an exhaustive list, and scholastic dishonesty may encompass other conduct, including any misconduct through electronic or computerized means. Scholastic dishonesty includes, but is not limited to, one or more of the following acts:

1. Cheating;
2. Collusion; and/or
3. Plagiarism.

Definitions of the scholastic dishonesty terms listed above are located in the current Student Code of Conduct.

In cases where an incident report has been filed for an alleged violation of scholastic dishonesty, the faculty member may either:

(1) delay posting a grade for the academic work in question until the case is finally adjudicated by the Dean of Students Office; or

(2) may enter a temporary placeholder grade of zero, along with an explanatory note, on the assignment(s) under review until the case is finally adjudicated by the Dean of Students Office.

~~will delay posting a grade for the academic work in question until the case is final~~.

A final grade for the course shall not be entered prior to a final resolution of the case by the Dean of Students Office. A student found responsible for a scholastic dishonesty offense(s) will receive an appropriate disciplinary penalty or penalties from the Dean of Students Office. The student may also receive an academic penalty in the course where the scholastic dishonesty took place. The faculty member will determine the appropriate academic penalty based on their syllabus policies and in compliance with law, which may include, but is not limited to, ~~range~~ ~~from~~ a grade of zero (0) on the assignment or ~~to~~ failing the course.

Student Code of Conduct Violations

The College District may initiate disciplinary proceedings for a student or program applicant who commits an offense as provided below. This list is not exhaustive but provides examples of the types of violations that may result in discipline:

1. Committing an act of scholastic dishonesty including, but not limited to, cheating, collusion, and/or plagiarism.
2. Conducting himself or herself in a manner that interferes with or disrupts the educational environment, orderly process of the College District, or lawful rights of others.
3. Committing any offense that violates the College District's Core Values.
4. Damaging, stealing, defacing, or destroying College District property, property belonging to a third party on a College District-sponsored trip, or property belonging to a College District student, faculty or staff member, or a campus visitor.
5. Theft, sabotage, destruction, distribution, or other use of the intellectual property of the College District or third parties without permission.
6. Knowingly giving false information in response to reasonable requests from College District officials.
7. Assaulting, threatening, abusing (physically, verbally, and/or sexually), or endangering in any manner the health or safety of a person at the College District, on College District property, or at a College District-sponsored event.

8. Violating the College District Student Code of Conduct; Board policies; laws; or administrative rules, regulations, and procedures (e.g., parking, guidelines for student events, registration of meetings and activities, use of College District facilities or the time, place, and manner of public expression).

9. Failing to comply with directions of College District officials and/or police acting in the performance of their duties.

10. Failing to notify College District officials of a change in residency status or current address.

11. Being convicted of an indictable offense under either municipal, state, or federal law that occurred on College District property or at an off-campus, College District-sponsored event.

12. Attempting to, or possessing, manufacturing, delivering, distributing, selling, purchasing, using, or being under the influence of, alcoholic beverages, illegal controlled substances (as defined in the Texas Controlled Substance Act), steroids, substances referred to as “designer drugs,” and inappropriately or illegally using over-the-counter medications, prescription medications, inhalants, herbal/“natural” euphoriants, and/or look-alike products (i.e., what is represented to be any of the above-listed substances) at the College District, on College District property, or while attending College District-sponsored activities on- or off-campus. [See FLBE]

13. Retaliating against another student, campus visitor, or staff or faculty member.

14. Discriminating against, harassing, committing sexual assault, committing dating violence, committing domestic violence, engaging in bullying, and/or stalking another student, campus visitor, or staff or faculty member, including, but not limited to, sexual, racial, and disability discrimination or harassment.

15. Creating an intimidating, hostile, or offensive educational environment.

16. Using, possessing, or displaying any location-restricted knives, clubs, knuckle devices, firearm silencers, or other prohibited weapons or devices, in violation of the law or College District policies and procedures, on College District property or at a College District-sponsored or -related activity, unless written authorization is granted in advance by the District President or designee. [See CHF]

17. Engaging in gang-related activity and/or organized criminal activity at any College District facility or grounds. Such actions will subject a student to disciplinary penalties, while a student involved in illegal acts may be arrested and face criminal prosecution.

18. Failing to secure, misusing, or sharing College-Wide Identification (CWID) numbers, College District email accounts, restricted course registration numbers (CRNs), or other restricted access codes or passwords.

19. Repeatedly violating College District policies, procedures, or guidelines and/or repeating less serious breaches of conduct.

20. Misusing College District technology and/or using computing systems to harass others (including, but not limited to, sending, distributing, posting, or displaying offensive or threatening material, and forging mail messages, and/or any violation of digital copyright laws resulting in demonstrable harm to the College District's network or disruption of classroom activities. These violations may result in the suspension of College District technology resource privileges and will be addressed as a formal disciplinary matter.

21. Gambling illegally in any form, at the College District, on College District property, or at any College District-sponsored activity.

22. Engaging in the disruptive use of electronic, digital media, or telecommunication, and/or wearable devices (e.g., phones, smart watches, Fitbits, Bluetooth devices, tablets, etc.) during classes, labs, or other College District learning environments. In addition, all electronic, digital media, telecommunication, and/or wearable devices must be completely turned off (not in silent or vibrate mode) while taking examinations and prior to entering the College District's Testing Centers.

23. Failing to demonstrate respect for the privacy rights of employees, other students, and visitors, not complying with all regulations and laws regarding the protection of confidential information, and not complying with all College District regulations regarding the use of cameras and recording devices.

24. Engaging in hazing at the College District, on College District property, or at any College District-sponsored activity.

25. Smoking or using any tobacco product or other electronic smoking device (including personal vaporizers) on College District property.

26. Forging, altering, or misusing College District documents or records.

27. Unlawfully interfering with the exercise of expressive activities in common outdoor areas by others as permitted by Board policies.

Hazing

Section 51.936 of the Texas Higher Education Code and Texas Education Code Chapter 37, Subchapter F, prohibits hazing at the College District, on College District property, or while attending College District-sponsored activities on- or off-campus. [See FLBC(LEGAL)] The College District Dean of Student Office will publish or distribute a list of organizations that have been disciplined for hazing or convicted for hazing on- or off-campus during the previous three years.