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

Information Security Officer

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

Information Security Program

The College President or designee shall 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 shall 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 College 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 College President or designee shall 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. Additionally, ~~T~~the College District must ~~subject~~ require the website or application to ~~a~~ undergo a vulnerability assessment and penetration test ~~before~~ prior to deployment and to complete, at a minimum, biannual vulnerability assessments and penetration tests thereafter to ensure continued compliance with established security standards.

Covered Social Media Applications

The College President or designee shall adopt procedures prohibiting the installation or use of a covered 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

Effectiveness of Policies, Procedures, and Practices

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

Biennial Information Security Plan

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

Information Security Assessment

In accordance with law, at least every two years, the College District shall submit the results of its information security assessment to DIR and, if requested, the office of the governor, lieutenant governor, and speaker of the house of representatives.

Security Incidents

By the College District

Generally

Security Breach and Cybersecurity Incident Notification

The College District shall assess the significance of a security incident and report it to DIR and law enforcement in accordance with law and, if applicable, DIR requirements.

Upon discovering or receiving notification of a breach of system security or a ~~security~~cybersecurity incident, as defined by law, the College District shall, upon confirmation of such breach or incident, disclose it ~~the breach or incident~~ to affected persons or entities in accordance with the time frames established by law.

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 website.
4. Publication through broadcast media.

By Vendors and Third Parties

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 law and administrative procedures.