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

Information Security Officer

The 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 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 ~~College District's~~ information resources owned, leased, or under the custodianship of the College District against unauthorized or accidental modification, destruction, or disclosure. The~~This~~ 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 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.

Website and Mobile Application Security

The District President or designee will adopt procedures addressing the~~also address accessibility,~~ 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.

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 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

Generally

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.

Security Breach Notification

Upon discovering or receiving notification of a breach of system security, the College District will disclose the breach 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.