

**SAM – INFORMATION SECURITY
(Office of Information Security)**

GOVERNING PROVISIONS
(Revised 6/14)

5300.2

Policy: As set forth in Government Code section [11549.3](#), state entities shall comply with the information security and privacy policies, standards and procedures issued by the California Information Security Office (CISO). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the CISO, state entities shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer/Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

Governing Provisions: Government Code section [11549.3](#) provides the CISO with the responsibility and authority to create, issue, and maintain policies, standards, and procedures; direct each state entity to effectively manage risk; advise and consult with each state entity on security issues; and ensure each state entity is in compliance with the requirements specified in the State Administrative Manual (SAM) Chapter 5300.

Government Code section [11549.3](#) also provides the CISO with the responsibility to coordinate the activities of state entity ISOs for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards. The CISO is also provided with the authority to conduct, or require to be conducted, independent security assessments or audits of any entity. The cost of such assessments or audits shall be funded by the state entity being assessed or audited.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

GOVERNING PROVISIONS

5300.2 (Cont. 1)

(Revised 6/14)

Many information security and privacy requirements are program specific; thus, the legal and regulatory requirements may vary from one program to another. For example, the laws governing security and privacy for health care programs differ from the laws governing energy programs. The following overarching laws, which affect the categorization, classification, protection, and dissemination of information, are applicable to most state entities:

1. [Article 1, Section 1](#), of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
2. The Information Practices Act of 1977 (Civil Code section [1798](#), et seq.) places specific requirements on each state entity in the collection, use, maintenance, and dissemination of information relating to individuals.
3. The California Public Records Act (Government Code sections 6250-6265) provides for the inspection of public records and authorizes specific exemptions for not disclosing certain records or portions of certain records.
4. The State Records Management Act (Government Code sections 14740-14770) provides for the application of management methods to the creation, utilization, maintenance, retention, preservation, and disposal of state records, including determination of records essential to the continuation of state government in the event of a major disaster. ([SAM sections 1601 through 1699](#) contain administrative regulations in support of the Records Management Act.)
5. The Comprehensive Computer Data Access and Fraud Act (Penal Code section [502](#)) affords protection to individuals, businesses, and governmental entities from tampering, interference, damage, and unauthorized access to computer data and computer systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.