

SAM – INFORMATION SECURITY
(Office of Information Security)

MINIMUM SECURITY CONTROLS

5300.5

(Revised 12/2019)

Policy: California has adopted the [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-53](#) as minimum information security control requirements to support implementation and compliance with the [Federal Information Processing Standards \(FIPS\)](#). Each state entity shall use the [FIPS](#) and [NIST SP 800-53](#) in the planning, development, implementation, and maintenance of their information security programs. Adoption of these standards will facilitate a more consistent, comparable, and repeatable approach for securing state assets; and, create a foundation from which standardized assessment methods and procedures may be used to measure security program effectiveness.

The CISO has also adopted additional standards and procedures to address more specific requirements or needs unique to California. These additional standards are referenced in the applicable policy section and maintained in the [Statewide Information Management Manual \(SIMM\)](#). Entities shall ensure their security control selections and tailoring, at a minimum, comply with the State-defined Security Parameters for NIST SP 800-53 (SIMM 5300-A) and the prioritization of their information security program development and implementation align with the Foundational Framework for Information Security (SIMM 5300-B).

Governing Provisions: [SAM Section 5100](#) requires state entities to use the [American National Standards Institute \(ANSI\)](#) and the [FIPS](#) standards in their information management planning and operations.

Implementation Controls: [ANSI](#); [FIPS](#); [NIST SP 800-53](#); [SIMM 5300-A](#) and [SIMM 5300-B](#)