State of California

Department of Technology

Information Security Program Management Standard

Statewide Information Management Manual – 5305-A

September 2025

Table of Contents

Document History **2**

Introduction **3**

Purpose 3

Scope 3

Compliance 3

Information Security Program Management **4**

Governance 4

Security Program Management 4

Information Security and Privacy Roles and Responsibilities **5**

Information Asset Categorization and Classification **19**

Information Classification 20

Information System Security Categorization 23

Critical System Reporting **24**

Policy, Standards, and Procedures Management **25**

Administrative Policies and Procedures 25

Operational and Technical Policies and Procedures 26

Questions **29**

Revision History

Revision	Date of Release	Owner	Summary of Changes
Initial Release	September 2013	California Information Security Office	Standard, procedure and instructions transferred from State Administrative Manual, Chapter 5300 to new standard
Minor Update	January 2018	Office of Information Security (OIS)	Office Name Change; SIMM 5330- B reference name change
Minor Updates	July 2022	OIS	Consistent with the Policy, Standards and Procedure Management section introduction and corresponding NIST controls added “and procedure” where missing; added additional examples for limitation on ISO designation carrying multiple roles; and “latest revision” for NIST SP 800-53 reference added for clarity.
Minor Update	December 2023	OIS	Updated GC 6250-6265 to 7920.000-7931.000
Minor Update	August 2025	OIS	Added roles and functions to Information Security and Privacy Roles and Responsibilities section, updated verbiage for clarity and reviewed content. Added a new section called "Critical System Reporting" (on page 24)
Minor Update	September 2025	OIS	Explicitly added organizational policy review/acceptance/approval as specific function of State Entity Head

Introduction

Purpose

Executive management within state entities must demonstrate a strong commitment to information security and risk management. Risk management should include a clear division of responsibilities among management, technical staff, and program personnel, with written documentation outlining specific roles and duties.

Security policies and procedures within the state entity must be thoroughly documented, and all staff members must be familiar with them.

This standard provides a framework for a top-down approach to establishing, implementing, and governing a state entity's Information Security Program (ISP). It ensures that those responsible for protecting information assets actively drive and nurture the program.

Scope

This standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions, as defined in Government Code Section 11546.1.

Compliance

As outlined in Government Code (GC) Section 11549.3, the Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and state entities, providing information security and privacy guidance, and ensuring compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their state entity.

Compliance may be reflected in audit findings and maturity scores. Non-compliance will be addressed according to the Office of Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

Information Security Program Management

Governance

Leadership, organizational structure, communications, relationships, and processes form the basis of information security governance.

Information security governance will ensure the following:

- Alignment of information security objectives with business strategy
- Effective risk management
- Optimized security investments
- Measurable program results

Security Program Management

Information security program management shall be based upon an appropriate division of responsibility among management, technical, and program staff, with written documentation of specific responsibilities.

This principle extends to acting roles and backups filling in for the key security personnel. Management must assign ownership of information assets, including each automated file or database used by the state entity.

Normally, responsibility for automated information resides with the manager of the state entity program that employs the information.

When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

1. Which program collected the information?
2. Which program is responsible for the accuracy and integrity of the information?

3. Which program budgets the costs incurred in gathering, processing, storing, and distributing the information?
4. Which program has the most knowledge of the useful value of the information?
5. Which program would be most affected, and to what degree, if the information were lost, compromised, delayed, or disclosed to unauthorized parties?

SAM Chapter 5300 provides the security and privacy policy framework that state entities must follow. The Federal Information Processing Standards (FIPS), the National Institute of Standards and Technology (NIST), Special Publication 800-53, and the California government's specific standards and procedures shall be used as the implementation control framework.

Using these standards will facilitate a more consistent, comparable, and repeatable approach to securing state assets and create a foundation from which standardized assessment methods and procedures may be used to measure the security program's effectiveness.

Information Security and Privacy Roles and Responsibilities

Each state entity shall ensure that the roles and responsibilities of information security and privacy are effectively established and carried out in their organizations.

Role	Responsibility (Task)	Specific Functions (Task)
Secretary/Director (or equivalent head of the state entity, herein after referred to as state entity head)	Responsible for: • Entity operations (including mission, functions, image, or reputation). • The protection and appropriate use of information assets held by the state entity. • Taking reasonable measures for implementation and maintenance of the program.	• Approve, accept, and assume accountability for all organizational policies. • On an annual basis, the head of each state entity must submit the following to the Office of Information Security (OIS): • A Designation Letter (SIMM 5330-A) identifying the designation of critical personnel, including a Chief Information Officer, Information Security

	• Understanding the state entity's RRPOAM and risk management strategy. • Ensuring compliance with information security and privacy requirements. • Ensuring designated personnel (Designees) possess the qualifications, authority, and management support to carry out their designated role and responsibility effectively. • Ensuring knowledge and understanding of any state entity partnerships including host/hosted and steward/client relationships.	Officer, Privacy Officer/Coordinator, and Technology Recovery Coordinator. • A Technology Recovery Program Certification (SIMM 5325-B) along with a copy of the state entity's current Technology Recovery Plan. • An Information Security and Privacy Program Compliance Certification (SIMM 5330-B) certifying that the state entity is in compliance with all requirements governing information security, risk state management, and privacy for the state entity's programs. • An Information Technology Cost Report (SIMM 55-B & 55-C) summarizing the entity's actual and projected IT costs.
Executive Management	Responsible for: • Establishing the governance body that will direct staff resources, funding, and the activities necessary to implement and maintain the information security program fully. • Effectively managing risk and achieving compliance with information security and privacy laws and regulations.	On an ongoing basis: • Be visibly committed to achieving information security program goals and objectives and practicing management. • Create a security and privacy-aware organizational culture. • Complete annual information security and privacy training
Agency Chief Information Officer (AIO)	Responsible for: • IT, including IT assets, projects, and infrastructure, through the	On an ongoing basis: • Be visibly committed to achieving information security program goals

	oversight and management of the CIO and development of Agency Enterprise Architectures. • Providing oversight, driving adoption of strategies, and reporting on cybersecurity risk to state entities. • Ensuring the creation and maintenance of Agency cybersecurity policies, standards, and procedures. • Ensuring the establishment and maintenance of information security and privacy programs. • Providing oversight and driving the adoption of risk mitigating strategies for departments within their agency. • Providing oversight, identifying, and implementing risk mitigation plans of action and milestones that mitigate and remediate risks across multiple departments within their agency. • Providing oversight and flex resources between departments within their agency for information security program resource gaps.	and objectives and practicing risk management. • Attend Information Technology Leadership Executive Council (ITEC). • Create a security and privacy-aware organizational culture. • Be informed of cybersecurity incidents. • Complete annual information security and privacy training.
Agency Chief Information Security Officer (AISO)	Responsible for: • The creation and maintenance of Agency cybersecurity policies, standards and procedures.	On an ongoing basis: • Attend Information Security Advisory Council (ISAC). • Complete the “ISO Basic Training” course

	• Coordination of OIS requirements and initiatives with state entity ISOs. • Informing and advising Agency leadership on cybersecurity risks, threats, and incidents. • Assisting with resource prioritization. • Reinforcing statewide cybersecurity culture. • Developing and exercising Agency strategy to leverage capabilities and resources across the Agency. • Establishing and maintaining information security and privacy programs. • Providing oversight and driving the adoption of risk mitigating strategies for departments within their agency. • Providing oversight, identifying and implementing risk mitigation plan of action and milestones that mitigate and remediate risks across multiple departments within their agency. • Providing oversight and flex resources between departments within their agency for information security program resource gaps.	offered by OIS, within the six months of designation. • Be visibly committed to achieving information security program goals and objectives and practicing risk management. • Create a security and privacy-aware organizational culture. • Attend the OIS-chaired ISO and Incident Response Bi-monthly meetings. • Not be assigned multiple designated roles or roles that present a conflict of interest, such as having direct responsibility for application development, information processing, technology operations, internal auditing functions, or state entity programs. • Complete annual information security and privacy training
Chief Information Officer (CIO)	Responsible for: • Overseeing the information technology portfolio and information technology services within	On an ongoing basis: • Be visibly committed to achieving information security program goals and objectives and

	his or her state entity through the operational oversight of information technology budgets of departments, boards, bureaus, and offices within the state entity. • Developing the enterprise architecture for the state entity, subject to the review and approval of the California Technology Agency, to rationalize, standardize, and consolidate information technology applications, assets, data, and procedures for all departments, divisions, and offices within the state entity. • Providing oversight, driving adoption of strategies, and reporting on cybersecurity risk to state entities. • Ensuring the creation and maintenance of state entity cybersecurity policies, standards, and procedures. • Ensuring the establishment and maintenance of information security and privacy programs.	practicing risk management. • Create a security and privacy-aware organizational culture. • Complete annual information security and privacy training
Information Security Officer (ISO)	Responsible for: • Manage and oversee the state entity's Information Security and Privacy Programs, ensuring the protection of the state entity's information assets. • Providing oversight, driving adoption of strategies, and reporting	On an ongoing basis: • Complete the "ISO Basic Training" course offered by OIS, within the first six months of designation. • Attend the OIS-chaired ISO and Incident Response Bi-monthly meetings.

	on cybersecurity risk to state entities. • Ensuring the creation and maintenance of state entity cybersecurity policies, standards, and procedures. • Coordination of OIS requirements and initiatives. • Informing and advising state entity leadership on cybersecurity risks, threats, and incidents. • Emphasizing cybersecurity management and strategic planning, driving the implementation of baseline cybersecurity capabilities, and attesting to their maturity. • Assisting with resource prioritization.	• Create a security and privacy-aware organizational culture. • Be informed of security incidents and assist in remediation. • Not be assigned multiple designated roles or roles that present a conflict of interest, such as having direct responsibility for application development, information processing, technology operations, internal auditing functions, or state entity programs. • Complete annual information security and privacy training.
Technology Recovery Coordinator (TRC)	Responsible for: • Working with the state entity's program management (business owners) and continuity planners to develop, test and maintain a technology recovery plan. • Representing the state entity in the event of a disaster or other event resulting in the severe loss of information technology systems capabilities. • Possessing the qualifications (education, training, skills, and knowledge) sufficient to effectively execute the duties and responsibilities of the position, including sufficient knowledge of	On an ongoing basis: • Complete the "ISO Basic Training" course offered by the OIS, within the first six months of designation. • Attend the OIS chaired TRC Bi- monthly meetings. • Not be assigned multiple designated roles or roles which present a conflict of interest, such as having direct responsibility for application development, information processing, technology operations, internal auditing functions, or for state entity programs.

	information management and information technology within the state entity to work effectively with the data centers and vendors in re- establishing information processing and telecommunications services after an event has occurred.	• Complete annual information security and privacy training.
Privacy Officer/Privacy Program Coordinator (occasionally referred to as the Disclosure Officer)	Responsible for: • Maintaining an ongoing privacy program, including an annual training component for existing and new personnel. • Ensuring the state entity complies with all of the provisions of the California Information Practices Act (Civil Code Section 1798 et seq.) and any other privacy-related legal requirements that may apply to the administration of the state entity's programs, including but not limited to, Government Code section 11019.9 and State Administration Manual 5310-5310.7.	On an ongoing basis: • Complete the "ISO Basic Training" course offered by OIS, within the first six months of designation. • Attend the OIS-chaired Privacy Bi-monthly meetings. • Not be assigned multiple roles designated roles or roles that present a conflict of interest, such as having direct responsibility for application development, information processing, technology operations, internal auditing functions, or state entity programs. • Complete annual information security and privacy training • Assist program management with conducting Privacy Impact Assessments • Assist program management, technical management, and the ISO with incident response when

		incidents involve personal information.
Information Technology (IT) Management	Responsible for: • Implementing the necessary technical controls to preserve the state entity's information assets' confidentiality, integrity, and availability. • Managing the risks associated with those assets. • Monitor and report any actual or attempted security incidents to the information security officer.	On an ongoing basis: • Be visibly committed to achieving information security program goals and objectives and practicing risk management. • Creating a security and privacy-aware organizational culture. • Complete annual information security and privacy training and ensure personnel supervised complete annual training.
Personnel Management	Responsible for: • Working closely with the information asset owners, program management, the ISO, and Privacy Officer/Privacy Program Coordinator to establish, implement and enforce information security and privacy program requirements. • Consulting the California Department of Human Resources.	On an ongoing basis: • Assist with the identification of security roles and responsibilities for all personnel to ensure they are informed of their roles and responsibilities for using state entity information assets, to reduce the risk of inappropriate use, and to establish a documented process to remove access when changes occur. • Implement employment history, fingerprinting and or criminal background checks on personnel who work with or have access to confidential, personal, or sensitive information or critical applications as necessary and within the state entity’s authority to do so.

		• Assist with ensuring state entity personnel receive security and privacy awareness training regarding user, state entity, and statewide security responsibilities and policies before being granted access to information assets and at least annually thereafter. • Assist with the receipt and maintenance of signed acknowledgments of security responsibility by all personnel. • Assist with transfer procedures that ensure access rights and permissions to state entity information assets are reviewed for appropriateness and reauthorized by program management when personnel are transferred within the state entity so that access to information assets is limited to what personnel need to perform their job-related duties. • Assist with termination procedures that ensure state entity information assets are not accessible to separated personnel.
Program Management (also often referred to as	Responsible for the following within their areas of program responsibility:	On an ongoing basis: • Be visibly committed to achieving information security program goals

Business Managers)	• Specify the business needs as expressed in terms of confidentiality, integrity, and availability requirements for information processes and systems (both manual and automated) used to administer state entity programs. • Working collaboratively with the ISO and Governing Body to develop and implement program-specific information handling policies, procedures, and practices. • Monitoring the security and use of information assets. • Ensuring program staff and other information users are informed of and carry out information security and privacy responsibilities.	and objectives and practicing risk management. • Creating a security and privacy-aware organizational culture. • Complete annual information security and privacy training and ensure personnel supervised complete annual training.
Information Asset Owners (often the Program Unit and Management affiliated with a particular program)	Responsible for the following within their areas of program responsibility: • Eliminating the unnecessary collection, use, and maintenance of personal information in state entity records. • Providing proper notice with the collection of personal information, as required by Civil Code Section 1798.17 and in accordance with the Privacy Statement and Notices Standard (SIMM 5310-A) • Subject to executive management review,	On an ongoing basis: • Coordinate these responsibilities with the state entity ISO and Privacy Officer/Privacy Program Coordinator. • Perform these responsibilities throughout the information security life cycle of the information asset until its proper disposal. • Complete annual information security and privacy training

	classifying information assets, including each record, file, or database for which it has ownership responsibility in accordance with the need for precautions in controlling access to and preserving the security and integrity of the information asset. • Defining precautions for controlling access to and preserving the security and integrity of information assets that have been classified as requiring such precautions. • Authorizing access to the information in accordance with the classification of the information and legitimate business need for access to the information. • Monitoring and ensuring compliance with all applicable laws, state entity and state security policies and procedures affecting the information. • Identify the level of acceptable risk for each information asset. • Reporting security incidents and filing Information Security Incident Reports with the OIS. See SAM Section 5340. NOTE: This is usually done through the ISO or the Privacy Officer. • Submitting a breach notification to the OIS for review and approval	

	before its dissemination or release to any individuals. • Monitoring and ensuring authorized users and custodians know and comply with these responsibilities.	
Designers/Developers of Information Systems and Applications	Responsible for: • Working collaboratively with the information asset owner, the ISO, and the privacy officer/coordinator for their state entity to identify and document system confidentiality, integrity, and availability requirements. • Ensuring system design and architecture are implemented to support security requirements and enforcement of security policies and procedures. • Applying secure coding standards and practices, which include adherence to the principle of least privilege, use of default deny protection schema, input validation, sanitizing data, threat modeling, defense in-depth strategy, and effective quality assurance techniques.	On an ongoing basis: • Coordinate with the information asset owner and the state entity ISO and Privacy Officer/Privacy Program Coordinator. • Complete annual information security and privacy training.
IT Personnel	Responsible for: • Working closely with the ISO in establishing and implementing a systematic process to prevent potential adversaries from obtaining confidential, sensitive, or personal information related to the state entity's planning and activities.	On an ongoing basis: • Implement and enforce the necessary technical controls to preserve the state entity's information assets' confidentiality, integrity, and availability. • Manage the risks associated with those assets.

		• Monitor for and report any actual or attempted security incidents to the Information Security Officer. • Maintain strong passwords, at least 15 characters, for all system administrator accounts. • Not use system administrator accounts for anything other than system administration functions. • Complete annual information security and privacy training.
Security Operations Personnel	Responsible for: • Working closely with the ISO in establishing and implementing a systematic process to prevent potential adversaries from obtaining confidential, sensitive, or personal information related to the state entity's planning and activities through: • Identification of confidential, sensitive, or personal information • Analysis of threats • Analysis of vulnerabilities • Assessment of risks • Application of appropriate countermeasures.	On an ongoing basis: • Monitor for and report any actual or attempted security incidents to the Information Security Officer. • Maintain strong passwords, at least 15 characters, for all system administrator accounts. • Complete annual information security and privacy training.
Custodians of Information	Responsible for: • Monitoring and ensuring compliance with all applicable laws, and state entity and state security policies and procedures affecting the information. • Complying with any additional security policies	On an ongoing basis: • Monitor for and report any actual or attempted security incidents to the Information Security Officer. • Complete annual information security and privacy training

	and procedures established by the information asset owner and the state entity ISO. • Advising the information asset owner and the state entity ISO of vulnerabilities that may threaten the information and of specific means of protecting that information. • Notifying the information asset owner and the state entity ISO of any actual or attempted violations of security policies, practices, and procedures.	
Information Asset Users	Responsible for: • Using state information assets only for state purposes. • Taking adequate steps to safeguard the confidential, personal, or sensitive information in your care from unauthorized view and access, use, modification, disposal, loss, or theft, whether paper records or electronic devices containing protected information such as a laptop or mobile device. • Limiting access and use of state information assets to that necessary to perform their assigned duties. • Not using authorized access capabilities to access, view, or obtain information that may be accessible but not necessary to perform their assigned duties.	On an ongoing basis: • Monitor for and report any actual or attempted security incidents to the Information Security Officer. • Complete annual information security and privacy training if applicable to the role.

	• Complying with applicable state laws and policies (including copyright and license requirements), as well as any additional security policies and procedures established by the owner of the information and the state entity ISO. • Notifying the information owner and the state entity ISO of any actual or attempted violations of security policies, practices, and procedures.	

The table above is not considered or intended to be an all-inclusive list. Each state entity must establish additional roles and responsibilities as deemed necessary to effectively manage risk and implement and manage their state entity's information security and privacy programs.

Information Asset Categorization and Classification

The categorization and classification of information assets is a prerequisite for determining the level of protection needed. Each information asset for which the state entity has ownership responsibility shall be inventoried and identified to include the following:

1. Description and value of the information asset.
2. Owner of the information asset.
3. Custodians of the information asset.
4. Users of the information asset.
5. Classification of information.

6. FIPS Publication199 categorization and level of protection (Low, Moderate, or High).
7. The importance of information assets in executing the state entity's mission and program function.
8. Potential consequences and impacts if the information asset's confidentiality, integrity, and availability were compromised.

Information Classification

Information classification is the characterization of information based on an assessment of legal and regulatory requirements and the potential impact that a loss of confidentiality, integrity, or availability of such information would have on organizational operations, organizational assets, individuals, other organizations, and possibly the nation.

Subject to executive management review, the program unit that is the designated owner of the information asset is responsible for determining whether it is to be classified as public or confidential and whether it contains personal and/or sensitive data. The information asset owner is responsible for defining special security precautions that must be followed to ensure the information asset's security (confidentiality, integrity, and availability).

The state's information assets, including paper and electronic records, automated files, and databases, are essential public resources that must be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion. Each state entity must classify each record, file, and database as either public or confidential using the following classification structure:

1. Public Information - information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act (GC Sections 7920.000- 7931.000) or other applicable state or federal laws.
2. Confidential Information - information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act

(GC Sections 7920.000- 7931.000) or has restrictions on disclosure in accordance with other applicable state or federal laws.

Sensitive Information and Personal Information, as defined below, may occur in Public Information and/or Confidential Information.

3. Sensitive Information - Information maintained by state entities that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher-than-normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of state entity financial transactions and regulatory.
4. Personal Information - information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. See Civil Code Section 1798.3.
    a. Notice-Triggering Personal Information - specific items or personal information (name plus Social Security Number, driver's license/California identification card number, financial account number, medical information, or health information) that may trigger a requirement to notify individuals if it is reasonably believed to have been acquired by an unauthorized person. See Civil Code Section 1798.29.
    b. Protected Health Information - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State laws require special precautions to protect from unauthorized use, access, or disclosure. See Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5.

c. Electronic Health Information - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164.

d. Personal Information for Research Purposes - personal information requested by researchers specifically for research purposes. Releases may only be made to the University of California or other non-profit educational institutions and in accordance with the provisions set forth in the law, including the prior review and approval by the Committee for the Protection of Human Subjects (CPHS) of the California Health and Human Services Agency before such information is released. See Civil Code Section 1798.24(t).

Records, files, and databases containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When confidential, personal, or sensitive information is contained in public records, procedures must be used to protect it from inappropriate disclosure. Such procedures include removing, redacting, or otherwise masking the information's confidential, sensitive, or personal portions, rendering them unrecoverable before a public record is released or disclosed.

While the state entity's need to protect data from inappropriate disclosure is essential, so is the need for the state entity to take necessary action to preserve the integrity of the data. Agencies must develop and implement procedures for access, handling, and maintenance of personal and sensitive information in accordance with the Privacy Individual Access Standard (SIMM 5310-B).

Once information is classified in accordance with the above-referenced structure, state entities shall use FIPS Publication 199 to further categorize it based on potential impact,

as described in the next section, to determine the applicable baseline security controls to be implemented.

Information System Security Categorization

Each state entity shall use the FIPS Publication 199 to categorize its information systems and determine the level of protection based on the information system security categorization process. FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a security breach (i.e., a loss of confidentiality, integrity, or availability). These are illustrated in the following table.

Potential Impact is…	If…	Examples
Low	The loss of confidentiality, integrity, or availability could have a limited adverse effect on organizational operations, assets, or individuals.	The loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could seriously adversely affect organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability might (i) cause significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals, that does not involve loss of life or serious life-threatening injuries.
High	The loss of confidentiality, integrity, or availability	The loss of confidentiality, integrity, or availability might: (i) cause severe degradation

Potential Impact is…	If…	Examples
	could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in significant damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Once the state entity completes the categorization process, it will use the appropriate baseline security controls from NIST Special Publication 800-53.

Critical System Reporting

State entities must include their critical systems in the Technology Recovery Plan (SIMM 5325-A) and conduct a thorough Cal-CSIRS NIST System Assessment. The results of NIST assessments must be documented in the state entity's RRPOAM.

Failure to address identified risks may impact audit and risk scores, potentially triggering the Policy Compliance and Enforcement Policy (SIMM 5330-H) enforcement. Additionally, it is essential to incorporate all security-related risks from all sources (internal and external) into the RRPOAM. Examples of risk sources and their relative findings include, but are not limited to, the following sources:

- Internal & External Assessments
- Internal & External Audits
- Independent Security Assessments
- Asset Scanning Vulnerability Reports
- Compliance Reviews

- Self-Assessments
- Asset Assessments

Policy, Standards, and Procedures Management

State entities shall implement internal administrative, operational, and technical policies and procedures to support the information security program's goals, objectives, and compliance.

Administrative Policies and Procedures

The state entity’s internal administrative policies and procedures shall include, at a minimum, the following:

1. Security planning policy and procedures which provide for the effective implementation of security controls.
2. Security awareness and training policy and procedure ensuring a well-trained workforce is employed as part of a defense-in-depth strategy to protect organizations against various threats targeting or leveraging personnel.
3. Contingency planning policies and procedures are part of an overall organizational program for achieving continuity of operations for mission/business functions.
4. Risk assessment policies and procedures that ensure the state entity is effectively managing risk.
5. System and services acquisition policy and procedures that identify audit events that are significant and relevant to the security of information systems and the environments in which those systems operate to meet the specific and ongoing audit needs.
6. Security assessment and authorization policy and procedure ensure residual risk is identified and accepted as authorized by state entity heads or their designees.

7. Audit and accountability policy and procedure which identifies the information security-related audit review, analysis, and reporting performed by the state entity, including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.
8. Acceptable use (rules of behavior) and disclosure policies and procedures that clearly delineate appropriate use and the limitations and restrictions associated with the use of state entity-owned information assets, including:
    a. Display of system use notification message or security banner.
    b. Email use, retention, forward and auto-response agents, and etiquette.
    c. Internet use, browsing, downloads, and etiquette

Social media technologies, when approved by the state entity, are properly monitored and managed, and their use is in compliance with the Social Media Standard (SIMM 66B).

Operational and Technical Policies and Procedures

The state entity's internal operational and technical policies and procedures shall include, at a minimum, the following:

1. Access control policy and procedure, which ensures the identification of authorized users and the specification of access privileges.
2. Identification and authentication policy and procedures for identifying and authenticating state entity users and devices.
3. Technology upgrade policy and procedures, which include, but are not limited to, timely operating system upgrades on servers, routers, and firewalls. The

policy and procedures must address appropriate planning and testing of upgrades and state entity criteria for deciding which upgrades to apply.

4. Security patches and security upgrade policies and procedures include but are not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy and procedures must address the application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied and how quickly.

5. Firewall configuration policy and procedures must require the creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or equipment reboots.

6. Server configuration policy and procedures must address all servers that interact with Internet, extranet, or intranet traffic. The policy and procedures must require creating and documenting a baseline configuration for each server, updating the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or equipment rebooting.

7. Server hardening policy and procedures must cover all servers within the department, not only those that fall within the jurisdiction of the department's IT area. The policy and procedures must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy and procedures must address and be consistent with the department's policy for making security upgrades and security patches.

8. Software management and licensing policy and procedures must address acquisition from reliable and safe sources, identification and maintenance of an inventory of software approved for use on state entity systems, and clearly state the department's policy about not using pirated or unlicensed software and the consequences for doing so.

9. Peer-to-peer technology policy and procedures must indicate that peer-to-peer technology use for any non-business purpose is strictly prohibited. This includes but is not limited to, the transfer of music, movies, software, and other intellectual property. The CIO and ISO must approve the business use of peer-to-peer technologies.

10. All personal, sensitive, or confidential information stored on portable electronic storage media (such as CDs, DVDs, tapes, portable hard drives, and thumb drives) and on portable computing devices (including laptops, netbooks, tablets, and smartphones) must adhere to encryption policies and procedures. This means that encryption or approved alternative security controls are required. Any alternatives to encryption must be assessed individually and must receive written approval from the state entity's Chief Information Officer (CIO) and Information Security Officer (ISO) after a thorough risk assessment.

11. Remote access policy and procedures requiring remote access or telework arrangements to adhere to the Telework and Remote Access Security Standard (SIMM 5360-A).

12. Data download policy and procedures require that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and security established for the original data file must be applied in the new environment.

13. System and communications protection policy and procedures.

14. Incident response policy and procedures, which must align with Incident Reporting and Response Instructions (SIMM 5340-A) and Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C)

15. Media protection policy and procedures that address media access, marking, storage, and transport security.

16. Physical and environmental protection policy and procedures that outline the state entity's facility access and environmental protection controls.

17. Data destruction policy and procedures.

Questions

Questions regarding the implementation of this standard may be sent to:

California Department of Technology

Office of Information Security

security@state.ca.gov