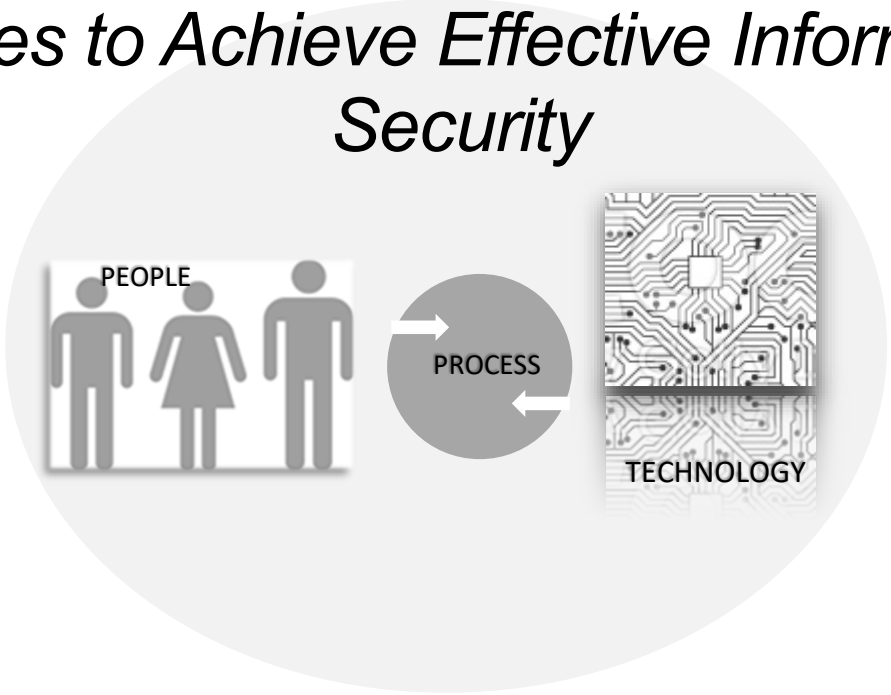
People, Process and Technology:

A Navigational Guide for Agency/State Entities to Achieve Effective Information Security



Office of Information Security
People, Process and Technology: A Navigational Guide for Agency/State Entities to Achieve Effective Information Security
September 2022

REVISION HISTORY

Revision	Date of Release	Owner	Summary of Changes
Initial Release	**November 2017**	**Office of Information Security (OIS)**	**New guidance document intended to help Agencies/state entities better understand the state policy and procedural requirements for establishment of effective enterprise-wide information security programs.**
Minor Update	**September 2022**	**OIS**	**Revised to include NIST 800-53, Rev 5.**

Introduction

Information security is an entity-wide responsibility and achieved through a combination of **people, process and technology.** The state's information assets, including its data processing capabilities, information technology infrastructure and data are an essential public resource. For many Agency/state entities, program operations would effectively cease in the absence of key computer systems. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. The non-availability of state information systems and resources can also have a detrimental impact on the state economy and the citizens who rely on state programs. Furthermore, the unauthorized acquisition, access, modification, deletion, or disclosure of information included in Agency/state entity files and databases can compromise the integrity of state programs, violate individual right to privacy, and constitute a criminal act.

This document is intended to help Agencies/state entities better understand the state policy and procedural requirements for establishment of effective enterprise-wide information security programs. For navigational ease, the policy requirements have been grouped in this document by categories aligned with **People, Process and Technology** so that entities can more easily understand what is needed to achieve state security objectives. Note: There may be some requirements that appear in multiple groupings. This was intentional.

For the complete published policy visit: *http://sam.dgs.ca.gov/TOC/5300.aspx*

Table of Contents

Policy	Requirement(s)	Reference(s)	Frequency
5305.3 Information Security Roles and Responsibilities	*All personnel have a role and responsibility in the proper use and protection of state information assets. Each state entity shall ensure the information security program roles and responsibilities identified in SIMM 5305-A are acknowledged and understood by all state entity personnel.*	Information Security Program Management Standard (SIMM 5305-A)	Initially, ongoing
5305.4 Personnel Management	*Each state entity must identify security and privacy roles and responsibilities for all personnel to ensure personnel are informed of their roles and responsibilities for using state entity information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur.*	Information Security Program Management Standard (SIMM 5305-A)	Initially, ongoing
5320 Training And Awareness For Information Security And Privacy	*Each state entity must establish and maintain an information security and privacy training and awareness program to assess the skills and knowledge of its personnel in relation to job requirements, identify and document training and professional development needs, and provide suitable training within the limits of available resources.*	NIST SP 800-53: Awareness and Training (AT)	Initially, ongoing
5320.1 Security And Privacy Awareness	*Each state entity shall provide basic security and privacy awareness training, which meets state requirements, to all information asset users (all personnel, including managers and senior executives) as part of initial training for new users and annually thereafter.*		Initially, annually
5320.2 Security And Privacy Training	*Each state entity shall determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security requirements of the state entity and the information assets to which personnel have access.*	Civil Code section 1798; NIST SP 800-53: Awareness and Training (AT)	Initially, annually

Policy	Requirement(s)	Reference(s)	Frequency
5320.3 Security And Privacy Training Records	*Each state entity shall document and monitor individual information security and privacy training activities including basic security and privacy awareness training and specific information system security training; and retain individual training records to support corrective action, audit and assessment processes. The ISO is responsible for ensuring that training content is maintained and updated as necessary.*	NIST SP 800-53: Awareness and Training (AT)	Initially, annually
5320.4 Personnel Security	*Each state entity shall establish processes and procedures to ensure that individual access to information assets is commensurate with job-related responsibilities, and individuals requiring access is commensurate with job-related responsibilities, and individuals requiring access to information assets sign appropriate user agreements prior to being granted access.*	NIST SP 800-53: Personnel Security (PS)	Initially, ongoing
5325.2 Technology Recovery Training	*Each state entity shall establish technology recovery training and exercises for personnel involved in technology recovery, to ensure availability of skilled staff.*	NIST SP 800-53: Contingency Planning (CP)	Initially, ongoing
5340.1 Incident Response Training	*Each state entity shall provide incident response training to information system users consistent with assigned roles and responsibilities.*	NIST SP 800-53: Incident Response (IR)	

Policy	Requirement(s)	Reference(s)	Frequency
5305.5 Information Asset Management	*Each state entity shall establish and maintain an inventory of all of its information assets, including information systems, information system components, and information repositories (both electronic and paper). The inventory must include categorization and classification of the information assets by program management, based on the Information Security Program Management Standard (SIMM 5305-A, California Public Records Act, Information Practices Act, FIPS Publication 199, and laws governing administration of the state entity's programs.*	Information Security Program Management Standard (SIMM 5305-A); Civil Code section 1798; NIST SP 800-53: Planning (PL); FIPS Publication 199	
5310.1 State Entity Privacy Statement And Notice On Collection	*Information asset owners shall be open about state entity information handling practices, including the purposes for which the state entity collects, uses, and discloses personal information of individuals. Each state entity Privacy Program Coordinator shall prepare, publish, and maintain a General Privacy Policy Statement and a Privacy Notice on Collection for each personal information collection.*	NIST SP 800-53; Privacy Statement and Notices Standard (SIMM 5310-A); Government Code section 11019.9	
5310.2 Limiting Collection	*Information asset owners shall collect the least amount of personal information that is required to fulfill the purposes for which it is being collected. Information asset owners shall obtain personal information only through lawful means and shall collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source.*	NIST SP 800-53	
5310.3 Limiting Use And Disclosure	*Information asset owners, custodians and users shall not disclose, use, or make available personal information collected from individuals for purposes other than those for which it was originally collected. (Exceptions for certain situations)*	Civil Code section 1798.24; NIST SP 800-53: Privacy Individual Access Standard (SIMM 5310-B)	
5310.4 Individual Access to Personal Information	*Each state entity shall ensure individuals are provided with information about their access rights and the procedures for exercising those rights.*	NIST SP 800-53;Privacy Individual Access Standard (SIMM 5310-B)	

Policy	Requirement(s)	Reference(s)	Frequency
5310.5 Information Integrity	*Information asset owners shall maintain all records with accuracy, relevance, timeliness, and completeness.*	NIST SP 800-53	
5310.6 Data Retention and Destruction	*Information asset owners shall retain and/or destroy records of personal information in accordance with the state entity's record retention and destruction policy and the Privacy Individual Access Standard (SIMM 5310-B). Information asset owners shall take reasonable steps to keep personal information only as long as is necessary to carry out the purposes for which the information was collected.*	NIST SP 800-53: Privacy Individual Access Standard (SIMM 5310-B)	
5310.7 Security Safeguards	*Information asset owners shall apply all applicable statewide and state entity information security laws, policies, standards, and procedures in order to protect personal information under the information asset owner's responsibility.*	NIST SP 800-53	
5315.2 System Development Lifecycle	*Each state entity shall manage its information assets using a documented SDLC methodology.*	NIST SP 800-53: System and Services Acquisition (SA)	
5315.3 Information Asset Documentation	*In conjunction with Records Management (SAM Chapter 1600) and Property Accounting (SAM Chapter 8600) requirements, each state entity shall ensure information security documentation is prepared and maintained as part of the overall documentation for all information assets.*	NIST SP 800-53: System and Services Acquisition (SA); SAM Chapters 1600 and 8600	
5350.1 Encryption	*End-to-end encryption or approved compensating security control(s) shall be used to protect confidential, sensitive, or personal information that is transmitted or accessed outside the secure internal network (e.g., email, remote access, file transfer, Internet/website communication tools) of the state entity, or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other mobile electronic devices.*	FIPS Publications 140-2 and 197; NIST SP 800-53: Access Control (AC); System and Communications Protection (SC)	

Policy	Requirement(s)	Reference(s)	Frequency
5365.2 Media Protection	*Each state entity shall safeguard media in digital and/or non-digital form from unauthorized access, use, modification or disposal, inside or outside of the state entity's control areas whether in storage or transport.*	NIST SP 800-53: Media Protection (MP)	
5365.3 Media Disposal	*Each state entity shall sanitize digital and non-digital media prior to disposal or release for reuse, in accordance with applicable standards and policies, including media found in devices such as hard drives, mobile devices, scanners, copiers, and printers.*	NIST SP 800-53: Media Protection (MP)	

Policy	Requirement(s)	Reference(s)	Frequency
5300.2 Governing Provisions	*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.*	Government Code Section 11549.3; California Constitution; California Information Practices Act; California Public Records Act; State Records Management Act; The Comprehensive Computer Data Access and Fraud Act	
5300.4 Definitions	*Each state entity shall use the information security and privacy definitions issued by the CISO in implementing information security and privacy policy in their daily operations.*	SAM 5300 Definitions	
5300.5 Minimum Security Controls	*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.*	FIPS; NIST SP 800-53	
5305 Information Security Program	*Each state entity is responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.*	NIST SP 800-53: Planning (PL); Program Management (PM);	

Policy	Requirement(s)	Reference(s)	Frequency
5305.1 Information Security Program Management	*Each state entity must provide for the proper use and protection of its information assets.*	NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A); Risk Register and Plan of Action and Milestones (SIMM 5305-B); Risk Register and Plan of Action and Milestones Worksheet (SIMM 5305-C)	
5305.2 Policy, Procedure and Standards Management	*Each state entity must provide for the protection of its information assets by establishing appropriate administrative, operational and technical policies, standards, and procedures to ensure its operations conform with business requirements, laws, and administrative policies, and personnel maintain a standard of due care to prevent misuse, loss, disruption or compromise of state entity information assets.*	NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A)	
5305.6 Risk Management	*Each state entity shall create a state entity-wide information security, privacy and risk management strategy which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the state entity's risk tolerance, and approaches for monitoring risk over time.*	NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A)	
5305.9 Information Security Program Metrics	*Each state entity shall establish outcome-based metrics to measure the effectiveness and efficiency of the state entity's information security program, and the security controls deployed.*	NIST SP 800-53: System and Services Acquisition (SA); Assessment, Authorization, and Monitoring (CA); Contingency Planning (CP)	

Policy	Requirement(s)	Reference(s)	Frequency
5310 Privacy	*State entity heads shall direct the establishment of an entity-specific Privacy Program. The Privacy Program shall ensure, and privacy coordinators shall confirm, that the requirements contained in the California Information Practices Act, this policy and the associated standards are adhered to by the state entity and its personnel.*	Civil Code section 1798; Fair Information Practice Principles (FIPPS); California Constitution Article 1, Section 1; Government Code section 11019.9; NIST SP 800-53	
5315.7 Software Usage Restrictions	*Each state entity shall ensure its Software Management Plan (SAM sections 4846.1 and 4846.2) addresses three installation requirements.*	SAM sections 4846.1 and 4846.2; NIST SP 800-53: Configuration Management (CM)	
5315.9 Security Authorization	*Consistent with the State Information Management Principles, Record of Decisions (SAM section 4800), each state entity shall establish a documented security authorization method which tracks official management decisions authorizing the operation of information assets and explicit acceptance of risks based on implementation of agreed-upon information security measures.*	SAM section 4800	
5330 Information Security Compliance	*Each state entity shall validate compliance with statewide information security policy, standards, and procedures as set forth in this Chapter, and the state entity's internal information security policies to verify that security measures are in place and functioning as intended.*	NIST SP 800-53: Assessment, Authorization, and Monitoring (CA)	
5330.2 Compliance Reporting	*Each state entity shall comply with reporting requirements as directed by the CISO. These reports include Designation Letter, Information Security and Privacy Program Compliance Certification, Technology Recovery Program Certification and/or Technology Recovery Plan, and the California Compliance and Security Incident Reporting System (CAL-CSIRS) Report.*	Designation Letter (SIMM 5330-A); Information Security and Privacy Program Compliance Certification (SIMM 5330-B); Technology Recovery Program Certification (SIMM 5325-B); California Compliance and Security Incident Reporting System (CAL-CSIRS); Risk Register and Plan of Action and Milestones (SIMM 5305-B); Risk Register and Plan of Action and Milestones Worksheet (SIMM 5305-C)	Varies by report.

Policy	Requirement(s)	Reference(s)	Frequency
5335.1 Continuous Monitoring	*Each state entity shall develop a continuous monitoring strategy and implement a continuous monitoring program.*	NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA); Assessment, Authorization, and Monitoring (CA)	

Policy	Requirement(s)	Reference(s)	Frequency
5340 Information Security Incident Management	*Each state entity must promptly investigate incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. All state entities are required to report information security incidents consistent with the security reporting requirements in this policy and manage information security incidents to determine the cause, scope, and impact of incidents to stop unwanted activity, limit loss and damage, and prevent recurrence.*	NIST SP 800-53: Incident Response (IR); Incident Reporting and Response Instructions (SIMM 5340-A); Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C)	
5340.2 Incident Response Testing	*Each state entity shall exercise or test their incident response capability to determine its effectiveness, document the results and incorporate lessons learned to continually improve the plan.*	NIST SP 800-53: Incident Response (IR)	
5340.3 Incident Handling	*Each state entity shall implement incident handling for information security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incident handling shall coordinate with business continuity planning activities (SAM section 5325).*	SAM section 5325; NIST SP 800-53: Incident Response (IR); Risk Register and Plan of Action and Milestones (SIMM 5305-B); Risk Register and Plan of Action and Milestones Worksheet (SIMM 5305-C)	
5340.4 Incident Reporting	*Each state entity shall follow the incident reporting procedures as described in SIMM 5340-A.*	NIST SP 800-53: Incident Response (IR); Incident Reporting and Response Instructions (SIMM 5340-A)	

Policy	Requirement(s)	Reference(s)	Frequency
5305.7 Risk Assessment	*Each state entity shall conduct an assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system/asset and the information it processes, stores, or transmits. Each state entity shall conduct a comprehensive risk assessment once every two years which assesses the state entity's risk management strategy for all three levels and documents the risk assessment results in a risk assessment report.*	NIST SP 800-53: Risk Assessment (RA)	Every two years
5315.5 Configuration Management	***Each state entity shall establish a documented process regarding controlled modifications to hardware, firmware, and software to protect the information asset against improper modification before, during, and after system implementation.***	NIST SP 800-53: Configuration Management (CM)	
5330.1 Security Assessments	*Each state entity shall perform security assessments to determine whether the security controls selected by the state entity are implemented correctly and working as intended to mitigate risk.*	NIST SP 800-53: Assessment, Authorization, and Monitoring (CA)	
5335 Information Security Monitoring	*Each state entity is responsible for continuous monitoring of its networks and other information assets for signs of attack, anomalies, and suspicious or inappropriate activities.*	NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA)	
5335.2 Auditable Events	***Each state entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained.***	NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA)	

Policy	Requirement(s)	Reference(s)	Frequency
5345 Vulnerability and Threat Management	*Each state entity shall continuously identify and remediate vulnerabilities before they can be exploited.*	NIST SP 800-53: Risk Assessment (RA); System and Services Acquisition (SA); System and Communications Protection (SC)	
5350 Operational Security	*Each state entity shall develop, implement, and document, disseminate, and maintain operational security practices and each state entity's security architecture shall align with best practices and documented security controls.*	NIST SP 800-53: System and Information Integrity (SI); System and Communications Protection (SC)	
5355.2 Security Alerts, Advisories, and Directives	*Each state entity shall continuously identify and remediate vulnerabilities before they can be exploited.*	NIST SP 800-53: Risk Assessment (RA); System and Services Acquisition (SA); System and Communications Protection (SC)	

Policy	Requirement(s)	Reference(s)	Frequency
5315.6 Activate Only Essential Functionality	*Each state entity shall configure information assets to provide only essential capabilities and functionality, and shall adhere to the principle of least privilege and restrict the use of unnecessary ports, protocols, and/or services to minimize the state entity's risk.*	NIST SP 800-53: Configuration Management (CM)	
5315.8 Information Asset Connections	*Each state entity shall carefully consider the risks that may be introduced when information assets are connected to other systems with different security requirements and security controls, both within the state entity and external to the state entity.* *Each state entity shall identify and maintain an inventory of its authorized information system connections with other state entities which establish authorized connections from information assets as defined by their authorization boundary, to other information systems.*	NIST SP 800-53: Access Control (AC)	
5350 Operational Security	*Each state entity shall develop, implement, and document, disseminate, and maintain operational security practices and each state entity's security architecture shall align with best practices and documented security controls.*	NIST SP 800-53: System and Information Integrity (SI); System and Communications Protection (SC)	
5355 Endpoint Defense	*Each state entity shall be responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft.*	NIST SP 800-53: System and Information Integrity (SI)	
5355.1 Malicious Code Protection	*Each state entity shall employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code.*	NIST SP 800-53: System and Information Integrity (SI)	

Policy	Requirement(s)	Reference(s)	Frequency
5360 Identity and Access Management	*Each state entity shall safeguard access to information assets by managing the identities of users and devices and controlling access to resources and data bases on a need-to-know basis throughout the identity lifecycle.*	NIST SP 800-53: System and Information Integrity (SI)	
5360.1 Remote Access	*Each entity shall establish, and document allowed methods of remote access to its information systems; establish usage restrictions and implementation guidance for each allowed remote access method; and monitor the information asset for unauthorized remote access. Allowed methods shall comply with the Telework and Remote Access Security Standard (SIMM 5360-A).*	NIST SP 800-53: Access Control (AC); Telework and Remote Access Security Standard (SIMM 5360-A)	
5360.2 Wireless Access	*Each state entity shall establish appropriate restrictions and implementation instructions for wireless access and enforce requirements for wireless connections to information systems. Each state entity shall also proactively search for unauthorized wireless connections including scans for unauthorized Wi-Fi access points.*	NIST SP 800-53: Access Control (AC); Telework and Remote Access Security Standard (SIMM 5360-A)	
5365 Physical Security	*Each state entity shall establish and implement physical security and environmental protection controls to safeguard information assets against unauthorized access, use, disclosure, disruption, modification or destruction.*	NIST SP 800-53: Physical and Environmental Protection (PE)	
5365.1 Access Control for Output Devices	*Each state entity shall control access to information system output devices, such as printers and facsimile devices, to prevent unauthorized individuals from obtaining the output.*	NIST SP 800-53: Physical and Environmental Protection (PE)	

Policy	Requirement(s)	Reference(s)	Frequency
5325 Business Continuity with Technology Recovery	*Each state entity shall ensure individuals with knowledge about business functions of the organization lead and participate in the business continuity planning. Note: The Business Continuity Plan must also address the Office of Emergency Services' (OES) continuity planning requirements.*	NIST SP 800-34; NIST SP 800-53: Contingency Planning (CP); OES Continuity Planning	
5325.1 Technology Recovery Plan	*Each state entity shall develop a TRP in support of the state entity's Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster. Each state entity must keep its TRP up-to-date and provide annual documentation for those updates to the CISO.*	NIST SP 800-34;NIST SP 800-53: Contingency Planning; Technology Recovery Plan Instructions (SIMM 5325-A); Technology Recovery Program Certification (SIMM 5325-B)	
5325.3 Technology Recovery Testing	*Each state entity shall test the TRP to determine its effectiveness and the state entity's readiness to execute the TRP in the event of a disaster. Each state entity shall initiate corrective actions and improvements to the TRP based upon deficiencies identified during testing and exercises.*	NIST SP 800-53: Contingency Planning	
5325.4 Alternate Storage and Processing Site	*Each state entity shall establish an alternate storage site, including the necessary agreements to permit the storage and recovery of backup information. Each state entity shall ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.*	NIST SP 800-53: Contingency Planning	
5325.5 Telecommunications Services	*Each state entity shall ensure they have alternate telecommunications services including necessary agreements to permit the resumption of information asset operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.*	NIST SP 800-53: Contingency Planning	

Policy	Requirement(s)	Reference(s)	Frequency
5325.6 Information System Backups	*Each state entity shall perform regularly scheduled backups of system and user-level information.*	NIST SP 800-53: Contingency Planning	

Policy	Requirement(s)	Reference(s)	Frequency
5315 Information Security Integration	*Each state entity is responsible for the integration of information security and privacy within the organization. This includes, but is not limited to, the designing of appropriate security controls in new systems, or systems that are undergoing substantial redesign, including both in-house and outsourced solutions.*	SAM section 4800; NIST SP 800-53: System and Services Acquisition (SA)	
5315.4 System Developer Security Testing	*Each state entity shall require that system developers create and implement a security test and evaluation plan as part of the system design and build. When a contract is required, it shall specify the acceptance criteria for security test and evaluation plans and vulnerability remediation processes.*	NIST SP 800-53: System and Services Acquisition (SA)	
5315.5 Configuration Management	*Each state entity shall establish a documented process regarding controlled modifications to hardware, firmware, and software to protect the information asset against improper modification before, during, and after system implementation.*	NIST SP 800-53: Configuration Management (CM)	
5335.2 Auditable Events	*Each state entity shall ensure that information systems are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained.*	NIST SP 800-53: Audit and Accountability (AU); Physical and Environmental Protection (PE); Risk Assessment (RA)	
5305.8 Provisions for Agreements with State and Non-State Entities	*Each state entity shall ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state.*	NIST SP 800-53: System and Services Acquisition (SA); FIPS Publication 199	
5315.1 System and Services Acquisition	*Each state entity shall determine the information security requirements (confidentiality, integrity, and availability) for its information assets in mission/business process planning; determine, document and allocate the resources required to protect the information assets as part of its capital planning and investment control process; and, establish organizational programming and budgeting documentation.*	NIST SP 800-53: System and Services Acquisition (SA)	

Policy	Requirement(s)	Reference(s)	Frequency
5315.2 System Development Lifecycle	*Each state entity shall manage its information assets using a documented SDLC methodology.*	NIST SP 800-53: Systems and Services Acquisition (SA)	