State of California

California Department of Technology

Office of Information Security

Information Security Program Management Standard

SIMM 5305-A

July 2022

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.**

TABLE OF CONTENTS

INTRODUCTION

State entity executive management must be visibly committed to information security and the practice of risk management. Risk management must be based upon an appropriate division of responsibility among management, technical, and program staff, with written documentation of specific responsibilities. State entity security policies and procedures must be fully documented, and state entity staff must be knowledgeable about those policies and procedures. This standard identifies the framework for a top-down executive management approach to establish, implement and govern the information security program. A top-down approach ensures the personnel responsible for and ultimately accountable for the protection of information assets are driving and cultivating the program.

INFORMATION SECURITY PROGRAM MANAGEMENT

Governance

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

1. Alignment of information security objectives with business strategy
2. Effective risk management
3. Optimized security investments
4. 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. Management must assign ownership of information assets, including each automated file or data base 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?

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

INFORMATION SECURITY AND PRIVACY ROLES AND RESPONSIBILITIES

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

Role	Responsibility	Specific Functions
Secretary/Director (*or equivalent head of the state entity, herein after referred to as state entity head*)	Responsible for: 1. Entity operations (including mission, functions, image, or reputation). 2. The protection and appropriate use of information assets held by the state entity. 3. Taking reasonable measures for implementation and maintenance of the program. 4. Ensuring compliance with information security and privacy requirements. 5. Ensuring designated personnel (Designees) possess the qualifications, authority, and management support to effectively carry out their designated role and	On an annual basis the head of each state entity must submit the following to the Office of Information Security (OIS): 1. A Designation Letter (SIMM 5330-A) identifying the designation of critical personnel, including a Chief Information Officer, Information Security Officer, Privacy Officer/Coordinator, and Technology Recovery Coordinator. 2. A Technology Recovery Program Certification (SIMM 5325-B) along with a copy of the state entity's current Technology Recovery Plan. 3. 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,

Role	Responsibility	Specific Functions
	responsibility.	in compliance with all requirements governing information security, risk state management, and privacy for the entity's programs.
Executive Management	Responsible for: 1. Establishing the governance body that will direct staff resources, funding and the activities necessary to fully implement and maintain the information security program. 2. Effectively managing risk and achieve compliance with information security and privacy laws and regulations.	On an ongoing basis be: 1. Visibly committed to the achievement of information security program goals and objectives and the practice of risk management. 2. Creating a security and privacy aware organizational culture.

Chief Information Officer	Responsible for: 1. Overseeing the information technology portfolio and information technology services within his or her state entity through the operational oversight of information technology budgets of departments, boards, bureaus, and offices within the state entity. 2. Developing the enterprise architecture for his or her state entity, subject to the review and approval of the California Technology Agency, to rationalize, standardize, and consolidate information technology applications, assets, and data, and procedures for all departments, divisions and offices within the state entity.	

Role	Responsibility	Specific Functions
Information Security Officer (ISO)	Responsible for: 1. Management and oversight of the state entity's Information Security Program ensuring protection of the state entity's information assets and state entity compliance with state information security policies, standards, and procedures. 2. Possessing the qualifications (education, training, skills, and knowledge) sufficient to effectively execute the duties and responsibilities of the position.	The ISO must: 1. Complete the "ISO Basic Training" course offered by the OIS, within the first three months of designation. 2. Attend the OIS chaired ISO Bi-monthly meetings. 3. Not be assigned multiple 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; or not be assigned multiple designee roles without added staff support to ensure the responsibilities of each designee role are effectively carried out.
Technology Recovery Coordinator	Responsible for: 1. Working with the state entity's program management (business owners) and continuity planners to develop, test and maintain a technology recovery plan. 2. Representing the state entity in the event of a disaster or other event resulting in the severe loss of information technology systems capability.	

Role	Responsibility	Specific Functions
	3. Possessing the qualifications (education, training, skills, and knowledge) sufficient to effectively execute the duties and responsibilities of the position, including sufficient knowledge of 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.	
Privacy Officer/Privacy Program Coordinator *(occasionally referred to as the Disclosure Officer)*	Responsible for: 1. Maintaining an ongoing privacy program, including an annual training component for existing and new personnel. 2. 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 which may be applicable 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.	The Privacy Officer/Privacy Program Coordinator must: 1. Assist program management with conducting Privacy Impact Assessments 2. Assist program management, technical management, and the ISO with incident response when incidents involve personal information.

Role	Responsibility	Specific Functions
Information Technology (IT) Management	Responsible for: 1. Implementing the necessary technical controls to preserve the confidentiality, integrity and availability of the state entity's information assets. 2. Managing the risks associated with those assets. 3. Monitoring for and reporting to the Information Security Officer any actual or attempted security incidents.	
Personnel Management	Responsible for: 1. 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.	Personnel Management must: 1. Assist with 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 the establishment of a documented process to remove access when changes occur. 2. Implement employment history, fingerprinting and or criminal

Role	Responsibility	Specific Functions
	2. Consulting the California Department of Human Resources.	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. 3. Assist with ensuring state entity personnel receive security and privacy awareness training with respect to user, state entity, and statewide security responsibilities and policies before being granted access to information assets, and at least annually thereafter. 4. Assist with the receipt and maintenance of signed acknowledgments of security responsibility by all personnel. 5. 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 an employee is transferred within the state entity, so that access to information assets is limited to that which is needed by the employee in the performance of their job-related duties. 6. Assist with termination procedures that ensure state entity information assets are not accessible to separated personnel.

Program Management *(also often referred to as Business Managers)*	Responsible for the following within their areas of program responsibility: 1. Specifying 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. 2. Working collaboratively with the ISO and Governing Body to develop and implement program specific information handling policies, procedures and practices. 3. Monitoring the security and use of information assets. 4. Ensuring that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.	

Role	Responsibility	Specific Functions
Information Asset Owners *(often the Program Unit and Management affiliated with a particular program)*	Responsible for the following within their areas of program responsibility: 1. Eliminating the unnecessary collection, use and maintenance of personal information in state entity records. 2. 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) 3. Subject to executive management review, 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.	Information Asset Owners must: 1. Coordinate these responsibilities with the state entity ISO and Privacy Officer/Privacy Program Coordinator. 2. Perform these responsibilities throughout the information security life cycle of the information asset until its proper disposal.

Role	Responsibility	Specific Functions
	4. Defining precautions for controlling access to and preserving the security and integrity of information assets that have been classified as requiring such precautions. 5. Authorizing access to the information in accordance with the classification of the information, and legitimate business need for access to the information. 6. Monitoring and ensuring compliance with all applicable laws, and state entity and state security policies and procedures affecting the information. 7. Identifying for each information asset the level of acceptable risk. 8. Reporting security incidents and filing Information Security Incident Reports with the California Information OIS. See SAM Section 5360. NOTE: This is usually done through the ISO or the Privacy Officer.	

Role	Responsibility	Specific Functions
	9. Submitting a breach notification to the OIS for review and approval prior to its dissemination or release to any individuals. 10. Monitoring and ensuring authorized users and custodians are aware of and comply with these responsibilities.	
Designers/Developers of Information Systems and Applications	Responsible for: 1. Working collaboratively with the information asset owner and the ISO, and Privacy Officer/Coordinator for their state entity to identify and document system confidentiality, integrity and availability requirements. 2. Ensuring system design and architecture is implemented to support security requirements and enforcement of security policies. 3. Applying secure coding standards and practices which include adherence to the principle of least privilege, use of a default deny protection schema, input validation, sanitizing data, threat modeling, defense in depth strategy, and effective quality assurance techniques.	

Role	Responsibility	Specific Functions
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.	IT Personnel must: Implement and enforce the necessary technical controls to preserve the confidentiality, integrity and availability of the state entity's information assets. Manage the risks associated with those assets. Monitor for and report to the Information Security Officer any actual or attempted security incidents. Maintain strong passwords, at least 15 characters, for all system administrator accounts. Not use system administrator accounts for anything other than system administration functions.
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	

Role	Responsibility	Specific Functions
	and activities through: 1. Identification of confidential, sensitive, or personal information; 2. Analysis of threats; 3. Analysis of vulnerabilities; 4. Assessment of risk; and 5. Application of appropriate countermeasures.	
Custodians of Information	Responsible for: 1. Monitoring and ensuring compliance with all applicable laws, and state entity and state security policies and procedures affecting the information. 2. Complying with any additional security policies and procedures established by the information asset owner and the state entity ISO. 3. Advising the information asset owner and the state entity ISO of vulnerabilities that may present a threat to the information and of specific means of protecting that information. 4. Notifying the information asset owner and the state entity ISO of any actual or attempted violations of security policies, practices and procedures.	

Role	Responsibility	Specific Functions
Information Asset Users	Responsible for: 1. Using state information assets only for state purposes. 2. 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. 3. Limiting access and use of state information assets to that which is necessary to the performance of their assigned duties. 4. Not using authorized access capabilities to access, view or obtain information which may be accessible, but not necessary to the performance of their assigned duties. 5. Complying with applicable state laws and policies (including copyright and license requirements), as well as any additional security policies and	

Role	Responsibility	Specific Functions
	Procedures established by the owner of the information and the state entity ISO. 6. Notifying the owner of the information 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 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. Federal Information Processing Standards (FIPS) Publication199 categorization and level of protection (Low, Moderate, or High).
7. Importance of information asset to the execution of the state entity's mission and program function.
8. Potential consequences and impacts if confidentiality, integrity and availability of the information asset 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 a and information asset is responsible for making the determination as to whether that information asset 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 security (confidentiality, integrity and availability) for the information asset.

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 (Government Code Sections 6250-6265) 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 (Government Code Sections 6250-6265) 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 agencies 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 actions.

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 CodeSection 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 the removal, redaction or otherwise masking of the confidential, sensitive or personal portions of the information, rendering it unrecoverable, before a public record is released or disclosed.

While the need for the state entity to protect data from inappropriate disclosure is important, 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 Information Asset Handling Standard (SIMM 5310-B).

Once information is classified in accordance with the above referenced structure, state entities shall use the FIPS Publication 199 to further categorize its information 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 breach of security (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 be expected to have a **limited** adverse effect on organizational operations, organizational 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 is able to 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 be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to 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 could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability might: (i) cause a severe degradation 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 major 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 set of baseline security controls from the latest revision of the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53.

POLICY, STANDARDS AND PROCEDURES MANAGEMENT

State entities shall implement internal administrative, operational and technical policies and procedures to support information security program goals and 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 which ensures a well-trained workforce is employed as part of a defense-in-depth strategy to protect organizations against a variety of threats targeting or leveraging personnel.
3. Contingency planning policy and procedures which is part of an overall organizational program for achieving continuity of operations for mission/business functions.
4. Risk assessment policy and procedures which ensure the state entity is effectively managing risk.
5. System and services acquisition policy and procedures which identify audit events that are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet the specific and ongoing audit needs.
6. Security assessment and authorization policy and procedure which ensure residual risk is identified, and has been 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 which 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
    d. Social media technologies, when approved by the state entity, is properly monitored and managed and 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 procedures which ensure 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 includes, but is not limited to timely operating systemupgrades on servers, routers, and firewalls. The policy and procedures must address appropriate planning and testing of upgrades, in addition to state entity criteria for deciding which upgrades to apply.
4. Security patches and security upgrade policy and procedures, which includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy and procedures must address 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, which must require 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 changedduring software modifications or rebooting of the equipment.
6. Server configuration policy and procedures, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy and procedures must require creation anddocumentation of a baseline configuration for each server, updates of the documentationfor all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
7. Server hardening policy and procedures, which 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 includethe process for making changes based on newly published vulnerability information as itbecomes 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 software licensing policy and procedures, which must address acquisitionfrom reliable and safe sources, identification and maintenance of an inventory of software approved for use on state entity systems, and must 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, which must indicate peer-to-peer technology use for any non-business purpose is strictly prohibited. This includes, but is not limited to, transfer ofmusic, movies, software, and other intellectual property. Business use of peer-to-peer technologies must be approved by the CIO and ISO.

10. Encryption policy and procedures requiring encryption or approved compensating security control(s), is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs, DVDs, tapes, portable hard

    drives, and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers, netbooks, tablets, and smart phones). Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the state entity CIO and ISO, after a thorough risk assessment.
11. Remote access policy and procedures requiring any remote access or telework arrangements to adhereto the Telework and Remote Access Security Standard (SIMM 5360-A).
12. Data download policy and procedures requiring that if a data file is downloaded to a mobile device ordesktop computer from another computer system, the specifications for information integrity and security which have been 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 which address media access, marking, storage and transport security.
16. Physical and environmental protection policies and procedures which outline the state entity's facility access and environmental protection controls.
17. Data destruction policy and procedures.