

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

Note: Effective January 1, 2008, the Office of Information Security (Office) restructured and renumbered the content and moved it from SAM Sections 4840 – 4845 to SAM Sections 5300 – 5399. See also the Office's Government Online Responsible Information Management (GO RIM) Web site at www.infosecurity.ca.gov for statewide authority, standards, guidance, forms, and tools for information security activities.

CHAPTER 5300 INDEX

INTRODUCTION	5300
STATUTORY PROVISIONS	5300.1
APPLICABILITY	5300.2
AGENCY RESPONSIBILITIES	5300.3
DEFINITIONS	5300.4
RISK MANAGEMENT	5305
RISK ANALYSIS	5305.1
AGENCY RISK MANAGEMENT PROGRAM	5305.2
POLICY, STANDARDS, AND PROCEDURE MANAGEMENT	5310
ORGANIZING INFORMATION SECURITY	5315
AGENCY MANAGEMENT RESPONSIBILITIES	5315.1
AGENCY DESIGNATIONS	5315.2
ASSET PROTECTION	5320
OWNERSHIP OF INFORMATION	5320.1
RESPONSIBILITY OF OWNERS OF INFORMATION	5320.2
RESPONSIBILITY OF CUSTODIANS OF INFORMATION	5320.3
RESPONSIBILITY OF USERS OF INFORMATION	5320.4
CLASSIFICATION OF INFORMATION	5320.5
HUMAN RESOURCES SECURITY	5325
PHYSICAL AND ENVIRONMENTAL SECURITY	5330
COMMUNICATIONS AND OPERATIONS MANAGEMENT	5335

(Continued)

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

(Continued)

CHAPTER 5300 INDEX (Cont. 1)

INFORMATION INTEGRITY AND DATA SECURITY	5335.1
PERSONAL COMPUTER SECURITY	5335.2
ACCESS CONTROL	5340
INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE	5345
SOFTWARE LICENSING INTEGRITY PRACTICES	5345.1
CRYPTOGRAPHY	5345.2
INCIDENT MANAGEMENT	5350
INFORMATION SECURITY INCIDENT REPORTING REQUIREMENTS	5350.1
CRITERIA FOR REPORTING INCIDENTS	5350.2
INCIDENT FOLLOW-UP REPORT	5350.3
INCIDENTS INVOLVING PERSONAL INFORMATION	5350.4
DISASTER RECOVERY MANAGEMENT	5355
DISASTER RECOVERY PLANNING	5355.1
AGENCY DISASTER RECOVERY PLAN	5355.2
ADDITIONAL STATE DATA CENTER REQUIREMENTS	5355.3
COMPLIANCE	5360
COMPLIANCE SUMMARY	5360.1

INTRODUCTION **5300**
(Revised 03/11)

Information security means the protection of information and information systems, equipment, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information, regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction.

Government Code Section 11549 provides the Office of Information Security, within the California Technology Agency, with the responsibility and authority to create, issue, and maintain policies, standards, and procedures; direct state agencies to effectively manage security and risk; advise and consult with state agencies on security issues; and, ensure state agencies are in compliance with the requirements specified in the State Administrative Manual (SAM) Sections 5300 – 5399. These sections will continue to evolve as new policy is adopted.

SAM – INFORMATION SECURITY
(Office of Information Security)

STATUTORY PROVISIONS

5300.1

(Revised 03/11)

Pursuant to Government Code Section 11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures and filing requirements issued by the Office of Information Security. Additionally, the Office may conduct, or require to be conducted, independent security assessments or audits of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed or audited.

The primary provisions affecting the classification and dissemination of information under the control of California state agencies can be found in the State Constitution, in statute, and in administrative policy:

1. Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
2. The Information Practices Act of 1977 (Civil Code Section 1798, et seq.) places specific requirements on state agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
3. The California Public Records Act (Government Code Sections 6250-6265) provides for the inspection of public records.
4. The State Records Management Act (Government Code Sections 14740-14770) provides for the application of management methods to the creation, utilization, maintenance, retention, preservation, and disposal of state records, including determination of records essential to the continuation of state government in the event of a major disaster. (SAM Sections 1601 through 1699 contain administrative regulations in support of the Records Management Act.)
5. The Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502) affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.

See SAM Sections 5300 through 5399 and the Office's Government Online Responsible Information Management (GO RIM) Web site at www.infosecurity.ca.gov/ for statewide authority, standards, guidance, forms, and tools for information security activities.

APPLICABILITY

5300.2

(Revised 10/09)

The SAM Sections 5300 through 5399 shall apply to the following:

1. All state agencies, departments, offices, boards, commissions, institutions, and special organizational entities unless otherwise specifically exempted by law or state policy;
2. All categories of automated and paper information, including (but not limited to) records, files, and data bases; and,
3. Information technology facilities, software, and equipment (including personal computer systems) owned or leased by state agencies.

SAM – INFORMATION SECURITY
(Office of Information Security)

AGENCY RESPONSIBILITIES

5300.3

(Revised 10/09)

Each agency must provide for the proper use and protection of its information assets. Accordingly, each agency must perform the following:

1. Assign management responsibilities for information technology risk management, including the appointment of an Information Security Officer. See SAM Section 5315.
2. Provide for the integrity and security of automated and paper information, produced or used in the course of agency operations. See SAM Sections 5310 through 5350.
3. Provide for the security of information technology facilities, software, and equipment utilized for automated information processing. See SAM Section 5330.
4. Establish and maintain an information technology risk management program, including a risk analysis process. See SAM Section 5305.
5. Prepare and maintain an agency Disaster Recovery Plan. See SAM Section 5355.
6. Maintain a security and ongoing privacy program including an annual training component for all employees and contractors. Refer to Government Code 11019.9 and Civil Code 1798 et seq.
7. Comply with the state audit requirements relating to the integrity of information assets. See SAM Section 20000 et seq.
8. Comply with state reporting requirements. See SAM Section 5360.

Each state data center must carry out these responsibilities for those automated files, databases, and computer systems for which it has ownership responsibility. See SAM Sections 5320 and 5355.3.

DEFINITIONS

5300.4

(Revised 10/09)

Every State agency, department, and office shall use the information security and privacy definitions issued by the Office of Information Security and Privacy Protection in implementing information security and privacy policy and in their day to day operations. For example, use these definitions when interpreting and/or implementing State policies, creating and/or modifying departmental policies, and identifying, responding to, and reporting incidents.

The definitions are located on the Government Online for Responsible Information Management (Go RIM) Web site at <http://www.cio.ca.gov/OIS/Government/definitions.asp>.

SAM – INFORMATION SECURITY
(Office of Information Security)

RISK MANAGEMENT
(Revised 10/09)

5305

Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis (SAM Section 5305.1) and the initiation and monitoring of appropriate practices in response to that analysis through the agency's risk management program.

State agencies need to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure the physical security of these resources. Agencies shall also ensure that users, contractors, and third parties having access to state computerized information resources are informed of and abide by this policy and the agency security plan, and are informed of applicable state statutes related to computerized information resources.

Each agency that employs information technology must establish risk management and disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets. The state's information assets (its data processing capabilities, information technology infrastructure and data) are an essential public resource. For many agencies, 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 system and resources can also have a detrimental impact on the state economy and the citizens who rely on state programs. Furthermore, the unauthorized modification, deletion, or disclosure of information included in agency files and data bases can compromise the integrity of state programs, violate individual right to privacy, and constitute a criminal act.

RISK ANALYSIS
(Revised 10/09)

5305.1

As an essential aspect of its information technology security and risk management program, each agency that employs information technology must establish a risk analysis process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks. Specific risks that must be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of agency employees and outsiders; fire, flooding, and electric disturbances; and, loss of data communications capabilities.

The agency risk analysis process must identify and prioritize critical applications of information technology. When establishing priorities, agencies should consider that applications may become more critical as the period of unavailability increases and that processing cycles (i.e. monthly, quarterly or yearly) may have an impact upon the prioritization of applications. Agency risk management practices and disaster recovery planning must give priority to the establishment of policies and procedures to ensure the continued operation of these applications. See SAM Sections 5310 and 5355.

The risk analysis process must be carried out with sufficient regularity to ensure that the agency's approach to risk management is a realistic response to the current risks associated with its information assets. In general, the risk analysis process should be a cyclical process for most agencies. Agencies should complete the comprehensive risk analysis cycle at least every two years and whenever there has been a significant change in their use of information technology. This cycle ends with the preparation of a report documenting the risk assessment.

The risk analysis process should include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

RISK ANALYSIS

(Revised 10/09)

5305.1 (Cont. 1)

2. Identification of the agency information assets that are at risk, with particular emphasis on the applications of information technology that are critical to agency program operations. A critical application, from a statewide perspective, is an application that is so important to the state that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or, on the continuation of essential agency programs.
3. Identification of the threats to which the information assets could be exposed.
4. Assessment of the vulnerabilities, i.e., the points where information assets lack sufficient protection from identified threats.
5. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
6. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
7. Selection of cost-effective security management measures to be implemented.
8. Preparation of a report, to be submitted to the agency director and to be kept on file within the agency, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted by the agency.

AGENCY RISK MANAGEMENT PROGRAM

(Revised 10/09)

5305.2

The practice of information technology risk management within the agency must be based upon the results of the agency's risk analysis process. Obtaining resources for risk management is subject to the same technical, programmatic, and budgetary justification and review processes required for any information technology program. See SAM Section 4819.3.

The risk management practices implemented by the agency will vary depending upon the nature of the agency's information assets. Among the practices that must be included in each agency's risk management program are:

1. **Organizational and Management Practices**, see SAM Section 5315.
2. **Personnel Practices**, see SAM Section 5325.
3. **Physical Security Practices**, see SAM Section 5330.
4. **Information Integrity and Data Security Practices**, see SAM Section 5335.
5. **Personal Computer Security Practices**, see SAM Section 5335.
6. **Software Integrity Practices**, see SAM Section 5345.

SAM – INFORMATION SECURITY
(Office of Information Security)

POLICY, STANDARDS, AND PROCEDURE MANAGEMENT
(Revised 06/10)

5310

The purpose of information security policy, standards, and procedures are to establish and maintain a standard of due care to prevent misuse or loss of state agency information assets. Policy provides management direction for information security to conform with business requirements, laws, and administrative policies. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy. And procedures are the specific series of actions that are taken in order to comply with policies and standards.

Each agency must provide for the integrity and security of its information assets by establishing appropriate internal policies, standards, and procedures for preserving the integrity and security of each automated, paper file, or data base including:

1. Establishes and maintains management and staff accountability for protection of agency information assets.
2. Ensure the use of social media technologies is in compliance with the Social Media Standard (SIMM 66B).
3. Establishes and maintains processes for the analysis of risks associated with agency information assets.
4. Establishes and maintains cost-effective risk management practices intended to preserve agency ability to meet state program objectives in the event of the unavailability, loss or misuse of information assets.
5. Agreements with state and non-state entities to cover, at a minimum, the following:
 - a. Appropriate levels of confidentiality for the data based on data classification (see SAM Section 5320.5).
 - b. Standards for transmission and storage of the data, if applicable.
 - c. Agreements to comply with all state policy and law regarding use of information resources and data.
 - d. Signed confidentiality statements.
 - e. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
 - f. Agreements to notify the state data owners promptly if a security incident involving the data occurs.
6. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:
 - a. Technology upgrade policy, which includes, but is not limited to operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
 - b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy 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.
 - c. Firewall configuration policy, 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 changed during software modifications or rebooting of the equipment.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

POLICY, STANDARDS, AND PROCEDURE MANAGEMENT

5310 (Cont. 1)

(Revised 06/10)

- d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent, with the department's policy for making security upgrades and security patches.
 - f. Software management and software licensing policy, which must address acquisition from reliable and safe sources, and must clearly state the department's policy about not using pirated or unlicensed software.
 - g. Ensure that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Business use of peer-to-peer technologies must be approved by the CIO and ISO.
7. Requiring 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 which have been established for the original data file must be applied in the new environment.
8. Establishing policy requiring encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes. (See SAM Section 5345.2).

ORGANIZING INFORMATION SECURITY

5315

(Revised 10/09)

Agency 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. Agency security policies and procedures must be fully documented, and agency staff must be knowledgeable about those policies and procedures. This section identifies the framework management establishes for the implementation of information security. See SAM Section 5360 for Filing requirements.

SAM – INFORMATION SECURITY
(Office of Information Security)

AGENCY MANAGEMENT RESPONSIBILITIES
(Revised 10/09)

5315.1

Executive Management—The agency director has ultimate responsibility for information technology security, risk management, and privacy within the agency. Agency directors are responsible and shall take reasonable measures for implementation of, and compliance with, the state security policy and are accountable for the computerized information resources held by their agencies. Agency directors are responsible for the integrity of computerized information resources and the authorization of access to those resources. All agency employees share in this responsibility as well. On an annual basis the Director of each state agency must submit an Agency Designation Letter (SIMM Section 70A) designating critical personnel. See SAM Section 5360. Each year, the agency director must certify that the agency is in compliance with state policy governing information technology security, risk management, and privacy program by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). See SAM Sections 5305 and 5360. The Director must also transmit each year an updated copy of the agency's Disaster Recovery Plan with the Agency Disaster Recovery Plan Transmittal Letter (SIMM Section 70D), or Agency Disaster Recovery Plan Certification (SIMM Section 70B) to the Office. See SAM Sections 5355 and 5360.

Information Security Officer—Oversight responsibility at the agency level for ensuring the integrity and security of automated and paper files, databases, and computer systems must be vested in the agency Information Security Officer (ISO). The ISO is required to oversee agency compliance with policies and procedures regarding the security of information assets. The ISO must be directly responsible to the agency director for this purpose and be of a sufficiently high-level classification that he or she can execute the responsibilities of the office in an effective and independent manner. It is acceptable to create this reporting relationship on a functional basis rather than reorganize the department. To avoid conflicts of interest, the ISO (for agencies other than state data centers) should not have direct responsibility for information processing, technology operations, or for agency programs that employ confidential information.

Disaster Recovery Coordinator—Each agency must designate a Disaster Recovery Coordinator to represent the agency in the event of a disaster or other event resulting in the severe loss of IT systems capability. The designated individual must have sufficient knowledge of information management and information technology within the agency to work effectively with the data centers and vendors in re-establishing information processing and telecommunications services after an event has occurred. The name, title, business address, and phone number of the coordinator must be submitted to the Office with the agency's Disaster Recovery Plan, and annual Agency Designation Letter (SIMM Section 70A), as appropriate. See SAM Section 5360.

Technical Management—Agency information technology management is responsible for (1) implementing the necessary technical means to preserve the security, privacy, and integrity of the agency's information assets and manage the risks associated with those assets and (2) acting as a custodian of information per SAM Section 5320.3.

Program Management—Agency program managers are responsible (1) for specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) for ensuring that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.

The establishment of positions to meet agency information security responsibilities must be justified in accordance with established personnel and budgetary requirements.

SAM – INFORMATION SECURITY
(Office of Information Security)

AGENCY DESIGNATIONS
(Revised 10/09)

5315.2

Designation of Information Security Officer, Disaster Recovery Coordinator, and Privacy Program Coordinator - Due by January 31 of each year, or as designee changes occur. The director of each agency must designate and provide contact information for the agency's Information Security Officer (ISO), the Disaster Recovery Coordinator, and Privacy Program Coordinator using the Agency Designation Letter (SIMM Section 70A). Upon the designation of a new ISO, Disaster Recovery Coordinator, and/or Privacy Program Coordinator, the agency must submit an updated Agency Designation Letter to the Office within ten (10) business days.

ASSET PROTECTION
(Revised 10/09)

5320

Each agency must provide for the integrity and security of its information assets by identifying all automated files and data bases for which the agency has ownership responsibility, and ensuring that responsibility for each automated file or data base is defined with respect to the following:

1. Owners of the information within the agency.
2. Custodians of the information.
3. Users of the information.
4. Classification of information to ensure that each automated file or database is identified as to its information class in accordance with law and administrative policy.

OWNERSHIP OF INFORMATION
(Revised 10/09)

5320.1

Agency management must assign ownership of each automated file or data base used by the agency. Normally, responsibility for automated information resides with the manager of the agency 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 – INFORMATION SECURITY
(Office of Information Security)

RESPONSIBILITY OF OWNERS OF INFORMATION
(Revised 03/11)

5320.2

The responsibilities of an agency unit that is the designated owner of records (paper or electronic, including automated files, or databases) consist of:

1. Eliminating the unnecessary collection, use and maintenance of personal information in agency records.
2. Providing proper notice with the collection of personal information, as required by Civil Code Section 1798.17.
3. Classifying 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 record, file, or data base.
4. Defining precautions for controlling access to and preserving the security and integrity of records, files and data bases that have been classified as requiring such precautions.
5. Authorizing access to the information in accordance with the classification of the information and the need for access to the information.
6. Monitoring and ensuring compliance with all applicable laws, and agency and state security policies and procedures affecting the information.
7. Identifying for each record, file or data base the level of acceptable risk.
8. Reporting security incidents and filing Information Security Incident Reports with the Office of Information Security. See SAM Section 5360.
9. Submitting a breach notification to the Office 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.

The ownership responsibilities must be fulfilled throughout the life cycle of the record, file, or database, until its proper disposal. Program units that have been designated owners of records, files and databases must coordinate these responsibilities with the agency Information Security Officer.

RESPONSIBILITY OF CUSTODIANS OF INFORMATION
(Revised 10/09)

5320.3

The responsibilities of a custodian of records (paper or electronic, including automated files, or databases) consist of:

1. Monitoring and ensuring compliance with all applicable laws, and agency and state security policies and procedures affecting the information.
2. Complying with any additional security policies and procedures established by the owner of the information and the agency Information Security Officer.
3. Advising the owner of the information and the agency Information Security Officer of vulnerabilities that may present a threat to the information and of specific means of protecting that information.
4. Notifying the owner of the information and the agency Information Security Officer of any actual or attempted violations of security policies, practices and procedures.

SAM – INFORMATION SECURITY
(Office of Information Security)

RESPONSIBILITY OF USERS OF INFORMATION
(Revised 10/09)

5320.4

The responsibilities of a user of information consist of:

1. Using state information assets only for state purposes.
2. Complying with applicable laws and administrative policies (including copyright and license requirements), as well as any additional security policies and procedures established by the owner of the information and the agency Information Security Officer.
3. Notifying the owner of the information and the agency Information Security Officer of any actual or attempted violations of security policies, practices and procedures.

CLASSIFICATION OF INFORMATION
(Revised 10/09)

5320.5

Subject to executive management review, the agency unit that is the designated owner of a record (paper or electronic, including automated files, or databases) is responsible for making the determination as to whether that record, file, or database should be classified as public, or confidential, and whether it contains personal, and/or sensitive data. The owner of the record, file, or data is responsible for defining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of the information.

The state's 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 agency must classify each record, file, and database 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 other applicable state or federal laws.

Sensitive Information and Personal Information, as defined below, may occur in Public Information and/or Confidential Information. Records, files, and databases containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When confidential, sensitive or personal 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 before a public record is released or disclosed.

While the need for the agency to protect data from inappropriate disclosure is important, so is the need for the agency 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.

1. 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 agency financial transactions and regulatory actions.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

CLASSIFICATION OF INFORMATION

5320.5 (Cont. 1)

(Revised 10/09)

2. 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.
 - a. Notice-triggering personal information - specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. See Civil Code Sections 1798.29 and 1798.3.
 - 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. Information for Research Purposes – personal information requested by researchers specifically for research purposes. Any request for personal information must be reviewed and approved by the Committee for the Protection of Human Subjects (CPHS) of the California Health and Human Services Agency before such information is released. Releases may only be made to the University of California or other non-profit educational institutions. See Civil Code Section 1798.24(t).

HUMAN RESOURCES SECURITY

5325

(Revised 10/09)

Each agency is responsible to provide security roles and responsibilities to employees, contractors and third party users. This will ensure the users are informed of their roles and responsibilities for using agency information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include:

1. Employment history and/or background checks on employees who work with or have access to confidential or sensitive information or critical applications may be necessary for particular agencies. Agencies should contact the Department of Personnel Administration for specific rules and regulations relative to employment history or background checks.
2. Training of agency employees, contractors, and third parties with respect to individual, agency, and statewide security responsibilities and policies.
3. Signing of acknowledgments of security responsibility by all employees.
4. Termination procedures that ensure that agency information assets are not accessible to former employees.

SAM – INFORMATION SECURITY
(Office of Information Security)

PHYSICAL AND ENVIRONMENTAL SECURITY
(Revised 10/09)

5330

Physical Security Practices prevent unauthorized physical access, damage, and interruption to an agency's assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take the appropriate physical security measures to provide for:

1. Management control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by agency staff and outsiders.
2. Prevention, detection, and suppression of fires.
3. Prevention, detection, and minimization of water damage.
4. Protection, detection, and minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure.

COMMUNICATIONS AND OPERATIONS MANAGEMENT
(Revised 10/09)

5335

Agencies are responsible for the management and operation of their information processing facilities. The security program should identify and document the appropriate practices to ensure the integrity and security of the agency's information assets.

INFORMATION INTEGRITY AND DATA SECURITY
(Revised 10/09)

5335.1

Information which has been inappropriately modified or destroyed (by outsiders or employees) can adversely impact public policy or the rights of citizens. Consequently, the accuracy and completeness of information systems and the data maintained within those systems should be a management concern. Each agency must establish controls to ensure that data entered into and stored in its automated files and data bases are complete and accurate, as well as ensure the accuracy of disseminated information. Depending upon the nature of the information being protected and the threats to which it is subjected, additional measures may be required to ensure the integrity and security of automated files and databases can range from password protection to encryption.

PERSONAL COMPUTER SECURITY
(Revised 10/09)

5335.2

Information maintained in a personal computer system, including laptop computers and mobile devices, must be subjected to the same degree of management control and verification of accuracy that is provided for information that is maintained in other automated files. Files containing confidential or sensitive data (as defined in SAM Section 5320.5) should not be stored in personal computer systems unless the agency can demonstrate that doing so is in the best interest of the state and that security measures have been implemented to provide adequate protection. Proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data as defined in SAM Section 5320.5, must be approved by the agency's Information Security Officer (SAM Section 5315.1) before implementation. The Information Security Officer will determine that the proposal complies with all applicable provisions of the SAM dealing with information security and risk management (SAM Sections 5300 through 5399).

SAM – INFORMATION SECURITY
(Office of Information Security)

ACCESS CONTROL
(Revised 12/12)

5340

Agency management is responsible for ensuring the appropriate physical, technical, and administrative controls are in place to support proper access to agency information assets. These controls must be based on both business and security requirements to prevent and detect unauthorized access, and must, at a minimum, include the following controls.

1. Mobile, telework, and remote access controls include, but are not limited to the following:
 - a. Compliance with the Telework and Remote Access Security Standard (SIMM 66A).
 - b. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information, and information necessary for the support of agency critical applications.
 - c. Periodically changing dial-up access telephone numbers.
 - d. Auditing usage of dial-up communications and Internet access for security violations.

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE
(Revised 10/09)

5345

Each agency must provide for the integrity and security of its information assets throughout the System Development Life Cycle (SDLC) beginning at acquisition through development and maintenance, ensuring security becomes an integral component of the agency's information technology activities. Appropriately identified and implemented, integrity and security is a business enabler.

SOFTWARE LICENSING INTEGRITY PRACTICES
(Revised 10/09)

5345.1

Software must be fully licensed and obtained only from a reputable source. Obtaining system software, applications, and automated data files from user's groups, bulletin boards, the Internet, or other information services should be done only in accordance with department policy. See SAM Section 5310, Item 5, Subsection f.

CRYPTOGRAPHY
(Revised 10/09)

5345.2

Encryption, or equally effective measures, is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes.

For the purpose of this policy, the terms "confidential information" and "sensitive information" are defined in SAM Sections 5320.5, and, "personal information" is defined in three categories as follows:

1. Notice-triggering information (Civil Code Section 1798.29).
2. Protected health information (45 C.F.R. Section 160.103).
3. Electronic health information (45 C.F.R. Section 160.103).

Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the agency ISO.

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT MANAGEMENT

5350

(Revised 10/09)

Agency management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All agencies are required to report information security incidents consistent with the security reporting requirements in this policy.

Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

INFORMATION SECURITY INCIDENT REPORTING REQUIREMENTS

5350.1

(Revised 10/09)

Upon discovery of any incident that meets the defined criteria below, all agencies must immediately report the incident following the Agency Information Security Incident Notification and Reporting Instructions found in SIMM Section 65B and in this policy. The Security Incident Report, part of the State Information Management Manual, is available via the Office's website at www.infosecurity.ca.gov/. The report must be submitted to the Office within ten working days of the Agency's becoming aware of an incident involving the theft of such information, including information stolen in conjunction with the theft of a computer or data storage device.

CRITERIA FOR REPORTING INCIDENTS

5350.2

(Revised 10/09)

Incidents reported to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) include, but are not limited to, the following:

1. **State Data (includes electronic, paper, or any other medium).**
 - a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal. (See SAM Section 5320.5).
 - b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
 - c. Deliberate or accidental distribution or release of personal information by an agency, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
 - d. Intentional noncompliance by the custodian of information with his/her responsibilities. (See SAM Section 5320.3).
2. **Inappropriate Use & Unauthorized Access** - This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.
3. **Equipment** - Theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.
4. **Computer Crime** - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.
5. **Any other incidents that violate agency policy.**

SAM – INFORMATION SECURITY
(Office of Information Security)

INCIDENT FOLLOW-UP REPORT

5350.3

(Revised 10/09)

Each agency having ownership responsibility for the asset (SAM Section 5320.1) must complete an Agency Information Security Incident Report (SIMM Section 65C) for each incident. The report is signed by the agency's director, Information Security Officer, and Privacy Officer if needed. Submit the report to the Office within ten (10) business days from the date of notification.

Any incident involving personal identifying information may require the agency to notify the effected individuals and additional reporting may be necessary for agencies that must adhere to Health Insurance portability and Accountability Act (HIPAA) requirements. Refer to the California Office of HIPAA Implementation (CalOHI) Policy Memorandum 2006-77 which can be found on the CalOHI website at <http://www.ohi.ca.gov/>.

The Office may require that the agency provide additional information in conjunction with its assessment of the incident.

INCIDENTS INVOLVING PERSONAL INFORMATION

5350.4

(Revised 03/11)

Every agency that collects, uses, or maintains records containing personal information shall establish and maintain in its incident management plan, procedures for ensuring that any breach of security involving personal information, regardless of its medium (e.g., paper, electronic, verbal) are reported and handled in the most expeditious and efficient manner. The agency's procedures must be documented and address, at a minimum, the following:

1. **Agency Incident Response Team.** An agency's procedures shall identify the positions responsible for responding to a breach of personal information. An agency's response team must include, at a minimum, an escalation manager, the Program Manager of the program or office experiencing the breach, the Information Security Officer (ISO), the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy, the Public Information or Communications Officer, Legal Counsel, and a representative from the Office of Information Security. The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and driving the process to completion. Some incidents will require the involvement of others not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. If the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves state employee's personal information, the agency's Personnel Officer or Human Resource Manager should be involved. Furthermore, if the incident involves multiple agencies, the response team from each agency may be involved.
2. **Protocol for Internal Reporting.** An agency's procedures shall outline the method, manner, and progression of internal reporting, as to ensure that executive management is informed about breaches involving personal information, and the Agency Incident Response Team is assembled and the incident is addressed in the most expeditious and efficient manner.
3. **Protocol for Security Incident Reporting.** Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to the CHP's ENTAC at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will require specific information about the incident and will forward that information to the Office of Information Security and to the CHP Computer Crimes Investigation Unit (CCIU). An agency should inform the officer taking the report that the incident involves a personal information breach and the type of media involved (e.g., electronic, paper, both electronic and paper, etc.). Representatives from the Office of Information Security and CCIU will contact the agency as soon as possible following their receipt of the ENTAC report.

IMPORTANT: A report made to CHP, other law enforcement agencies, or the Office of Information Security outside of the ENTAC notification process by email or other means is NOT an acceptable substitute for the required report to ENTAC.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

INCIDENTS INVOLVING PERSONAL INFORMATION
(Revised 03/11)

5350.4 (Cont.1)

4. **Decision Making Criteria and Protocol for Notifying Individuals.** An agency's procedures shall include documentation of the methods and manner for determining when and how a notification is to be made. The procedures shall be consistent with and comply with applicable laws and state policies. At a minimum, an agency's procedures will address the following elements:
- a. Whether the notification is required by law.
 - b. Whether the notification is required by state policy.
 - c. Timeliness of notification.
 - d. Source of notice.
 - e. Content of notice.
 - f. Approval of notice prior to release.
 - g. Method(s) of notification.
 - h. Preparation for follow-on inquiries.
 - i. Other actions that agencies can take to mitigate harm to individuals.
 - j. Other situations when notification should be considered.

A more detailed description of these elements is set forth in the SIMM 65D-Security Breach Involving Personal Information: Requirements and Decision-Making Criteria for State Agencies (SIMM 65D).

5. **Notice to Affected Individuals.** Notice to individuals when a breach of unencrypted notice-triggering data elements occurs, regardless of the media involved (electronic or paper), and in accordance with criteria set forth above.
6. Office of Information Security's **Prior Review and Approval of Breach Notice.** The Office of Information Security provides review and approval of the breach notice prior to its release to any individual as set forth in SIMM 65D.

SAM – INFORMATION SECURITY
(Office of Information Security)

DISASTER RECOVERY MANAGEMENT

5355

(Revised 10/09)

Each agency must establish a Business Continuity Management Program that provides processes supported by executive management and resources to ensure the appropriate steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the agency has the ability to continue its essential functions during a business disruption or major catastrophic event. The program controls ensure that information is protected by providing for regular backup of automated files and databases, identifies and reduces risks, limits the consequences of the incident, and ensures the availability of information assets for continued business.

DISASTER RECOVERY PLANNING

5355.1

(Revised 10/09)

Disaster recovery planning (formerly known as operational recovery planning) provides for continuity of computing operations in support of critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly migration toward the resumption of all computing services within an agency following a business disruption. It is essential that critical IT services and critical applications be restored as soon as possible.

It is significant to recognize that no disaster recovery program is ever complete. All disaster recovery planning is based upon available knowledge and assumptions, and must be adapted to changing circumstances and business needs, as appropriate. Strategies, procedures, and resources must be adapted as often as necessary in order to recover critical applications. Recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

The disaster recovery planning process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. Agencies should consider the results of their risk analysis process and their business impact analysis when developing their Disaster Recovery Plan (DRP). See SAM Section 5305 for requirements regarding risk analysis. Each agency's process should culminate in a viable, fully documented, and tested DRP. See SIMM Section 65A for requirements and guidelines regarding disaster recovery.

To provide for recoverability of new systems, all agencies must include disaster recovery considerations and costs in project authority documents and budget proposals. See SAM Section 4900 et seq. and SIMM Section 20 for requirements and guidelines.

To improve the likelihood for the full recovery of key business processes, DRPs should be developed as part of a complete business continuity program which includes emergency response and business resumption plans.

SAM – INFORMATION SECURITY
(Office of Information Security)

AGENCY DISASTER RECOVERY PLAN
(Revised 12/12)

5355.2

Each state agency (including each state data center) must maintain a Disaster Recovery Plan (DRP) identifying the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plans for resuming operations following an unplanned disruption of those applications.

Each agency that employs the services of a state data center must develop an understanding of the existing service level agreement for recovery services, and its recovery plan must document the data center services that will be required during recovery.

Each agency must keep its DRP up-to-date and provide annual documentation for those updates to the Office. The annual requirements are:

1. Each agency must file a copy of its DRP and the Agency Disaster Recovery Program Certification (SIMM Section 70B) with the Office, in accordance with the Agency Disaster Recovery Plan Submission Schedule.
2. If the agency employs the services of a state data center, it must also provide the data center with either a full copy or a subset of its plan, containing enough information for the data center to recover the agency's systems and/or data. _____
3. Each agency DRP must cover, at a minimum, ten topic areas which are listed and described in the Disaster Recovery Plan Documentation for Agencies Preparation Instructions (SIMM Section 65A). If the agency has not developed a full business continuity plan, three supplemental DRP requirements must be included as directed in SIMM Section 65A. In addition, if the DRP does not follow the format in SIMM Section 65A, a cross reference sheet (see SIMM Section 70B) must be included with the update to indicate where information on each topic area can be found in the DRP.

It is important to adapt the detailed content of each plan section to suit the needs of the individual agency, with the understanding that DRPs are based upon available information so they can be adjusted to changing circumstances.

ADDITIONAL STATE DATA CENTER REQUIREMENTS
(Revised 10/09)

5355.3

Agencies that obtain services from a state data center may enter into a formal agreement for the data center to assume operational responsibility for backup and restoration of automated files and databases.

1. **Provision of Technical Security Services.** State data centers must offer their client agencies support services and technical capabilities that will ensure the protection of automated files and data bases under the custodial care of the data center at a level that is consistent with the requirements of the agency.
2. **Restoration of Telecommunications Services Following a Disaster.** State data centers and their client agencies are jointly responsible for restoration of telecommunications capabilities. Typically, the data center is responsible for telecommunications restoration from the point data leaves the agency site (by wire, optical fiber, microwave, or radio) or from the point communications lines enter a multiplexer, concentrator, controller, or front-end communications processor belonging to the data center.

SAM – INFORMATION SECURITY
(Office of Information Security)

COMPLIANCE
(Revised 10/09)

5360

All state agencies are required to comply with the information security and privacy policies, standards, and procedures issued by the Office and report and file the appropriate compliance documents as identified in this section. All agencies must adhere to the Information Security Reporting Requirements in the following sections.

COMPLIANCE SUMMARY
(Revised 12/12)

5360.1

Designation of Information Security Officer, Disaster Recovery Coordinator and Privacy Coordinator - Due by January 31 of each year, or as designee changes occur. Upon the designation of a new ISO, Disaster Recovery Coordinator, and/or Privacy Program Coordinator, the agency must submit an updated Agency Designation Letter to the Office within ten (10) business days using the Agency Designation Letter (SIMM Section 70A). See SAM Section 5315.1

1. **Agency Risk Management and Privacy Program Compliance Certification** - Due by January 31 of each year. The director of each agency must certify that the agency is in compliance with state policy governing information technology risk management and privacy program compliance by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). See SAM Section 5315.1. Per Government Code Section 11019.9, agencies are required to maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Civil Code Section 1798 et seq.) that includes, but is not limited to, assigning a designated individual to oversee the program.
2. **Disaster Recovery Plan** – Each agency must file a copy of its Disaster Recovery Plan (DRP) with the Agency Disaster Recovery Program Certification (SIMM Section 70B) with the Office by the due date outlined in the Agency Disaster Recovery Plan Submission Schedule. If the agency employs the services of a state data center, it must also provide the data center with a copy of its plan or subset of the relevant recovery information from the agency’s DRP. See SAM section 5355.1.
3. **Incident Follow-up Report** - Each agency having ownership responsibility for the asset (SAM Section 5320.1) must complete an Agency Information Security Incident Report (SIMM Section 65C) for each incident. The report must be submitted to the Office within ten (10) business days from the date of notification.

The Office may require that the agency provide additional information in conjunction with its assessment of the incident.

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

This page intentionally left blank.