California Office of
Information Security
& Privacy Protection

Information Security
Program Guide
For State Agencies

April 2008

Table of Contents

Introduction

The Information Security Program Guide was originally developed by a workgroup of state agency Information Security Officers (ISO) in March 2006 as a guide to assist agencies in developing an information security program or enhancing their existing program. It was formally adopted by the State Chief Information Officer's Information Technology (IT) Council in April 2007.

As outlined in the California State Information Technology Strategic Plan, dated November 2006, Goal 3, Objective 1, Action #1, required the IT Council's Security Committee to update the IT Security Program Guidelines. This revised version more closely considers the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002 (formally ISO/IEC 17799:2005) standards, which is being formally adopted as the State of California's information security standard. This Guide is also in alignment with the State Administrative Manual (SAM) information security requirements outlined in Sections 5300-5399.

This Guide is applicable to all state agencies and should be considered:

1) To further strengthen or aid in the development of an agency's information security program needed to protect the integrity, availability, and confidentiality of agency data and safeguard information assets and resources.
2) To identify processes and techniques that promotes secure communications and the appropriate protection of information among agencies.
3) To establish a common information security program framework and format consistent across state agencies with different business needs.

This Guide identifies the twelve key components that should be considered by an agency when implementing, reviewing, or seeking to improve the value of its information security program. It is encouraged that these components be reviewed for applicability to an agency's business environment and compliance with existing laws and policies, and implemented as appropriate for each agency. Some agencies may not require all components, but where a component is applicable to an agency's program, it should be assessed for adoption and implementation. The key components are:

1. Risk Management
2. Policy Management
3. Organizing Information Security
4. Asset Protection
5. Human Resource Security
6. Physical and Environmental Security
7. Communication and Operations Management
8. Access Control
9. Information Systems Acquisition, Development and Maintenance
10. Incident Management
11. Disaster Recovery Management
12. Compliance

Together these components provide a framework for developing an agency's information security program, which must be a business core value. The components provide value to an agency's business by ensuring the reliability, integrity, and confidentiality of the information used by the agency and improves the robustness of an agency's technology infrastructure overall. A successful information security program supports business and aligns with the agency's mission, goals, and objectives.

To aid with the development of consistent, well designed security policies, this Guide includes a policy template along with a sample Acceptable Use Policy built on the template's recommended outline. Security policies are critical to the overall security program architecture and translate the concepts identified in the twelve core components into specific goals and objectives.

The Office of Information Security and Privacy Protection (OISPP) is grateful to the many agency ISOs and other security professionals who have provided their input to shape the content of this Guide.

A Suggested Implementation Strategy

Each agency must identify and implement security policies, standards, guidelines, processes, procedures, and best practices to protect its information assets while assuring its goals and objectives are being met. Given the diversity of business environments across the state, it is not practical to qualify all security best practices presented in this Guide or limit a security program to just this set of best practices. A large percentage of state agencies will find significant value in formally adopting the best practices listed in this Guide as part of their security program. The majority of these best practices are based upon the ISO 27002 (formally ISO 17799v2005) standards, the federal government's National Institute of Standards and Technology (NIST) Information Security Documents (for a complete listing of all documents refer to www.csrc.nist.gov/publications/CSD_DocsGuide.pdf), Federal Information Security Management Act (FISMA), and the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's report titled "The Internal Control – Integrated Framework" (see SAM Section 20050).

As outlined in SAM Sections 5300-5399, state agencies must have in place an effective risk management and information security program to ensure their information assets are properly protected. There is no easy solution to implementing an effective information security program. But, there are steps an agency can take to minimize the impact and ensure the program is implemented to fit the agency's business needs and align properly with its mission, goals, and objective and still be compliant with state policy and applicable laws, regulations, and statutes. It should be noted that an effective program cannot be established overnight and it will require a plan for continuous improvement over a period of years.

Typically, the ISO manages an agency's information security program. It is incumbent upon the ISO to understand organizational issues and their role within the activities of the agency. The ISO must keep abreast of technologies to ensure the appropriate controls are implemented and maintained. The ISO must understand the business process needs, assess internal and external risks, provide appropriate mitigation strategies, and stay current on laws and regulations. Additionally, the ISO must be directly responsible to the agency director to execute the responsibilities of the office in an effective and independent manner (refer SAM Section 5315.1).

The ISO's role has four types of information security activities:

- Planning – Identify an annual work plan to achieve security goals and objectives consistent with the agency's strategic plan.

- Developing – Lead in the development of information security policies, standards, guidelines, processes, and procedures.

- Managing – Conduct risk assessments, manage incidents, provide internal and external reporting, involvement in security awareness education and training, and

- Oversight – Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements (e.g., laws, regulations, statutes, state policy, etc.).

For details about the recommended role and responsibilities of an ISO, please review *The Guide for the Roles and Responsibilities of an Information Security Officer Within State Government.* It provides a state agency ISO general guidance and assistance in understanding his or her role and the responsibilities in developing and maintaining an effective information security program. It aligns with this Guide, but drills down into more detail about the important role of an agency ISO.

This Guide identifies the following nine steps to implementing an effective information security program or enhancing an existing one:

Step 1 – Form an internal information security governance structure

Governance is an essential component for the long-term strategy and direction of an organization within respect to the security policies and risk management program. Governance requires executive management's involvement, approval, and ongoing support. It also requires an organizational structure which provides the ISO with an appropriate venue to inform and advise executive, business, and IT management on security issues and acceptable risk levels. This can be accomplished through an existing executive committee or creation of a governance body within the agency and should be comprised of representatives from IT, human resources, legal, contracts, business services, program areas, privacy officer, operational recovery coordinator, and other key stakeholder areas.

The ISO should lead this effort or be an active participant in establishing and maintaining the governance structure. The committee, or governing body, should develop a charter, identify roles and responsibilities, and set goals and objectives. Members of the committee should meet as often as necessary to resolve ongoing issues, review new and revised security policies, standards, guidelines, processes, and procedures together as a team.

Refer to the *Organizing Information Security* section in this Guide for additional details.

Step 2 – Identify a baseline of the agency's inventory of information assets

Collect existing information security policies, standards, procedures, and guidelines. Determine if there are non-documented procedures and processes associated with information security in primary program areas like business services, human resources, and IT.

Collect any interagency agreements, contracts, memorandum of understandings, or service level agreements the agency may have in place related to responsibilities associated with information assets, such as the sharing or custodial responsibilities associated with confidential information or equipment.

Identify and gather inventory collections, which may include information assets (such as databases and files, training material, audit trails, operation or support procedures), software assets (such as application and system software, development tools, and utilities), physical assets (such as computer and communications equipment, removable media, and Uninterruptible Power Supplies[UPS]), and services (such as computing and communications services).

Review the agency's business strategies, mission, goals, and objectives. Review the agency's Business Continuity Plan, Continuity of Operations Plan/Continuity of

Government (COOP/COG), IT Strategic Plan, Disaster/Operational Recovery Plan, and any business area strategic plans to better understand the agency's business needs.

This effort will help develop a baseline, or understanding, of what is currently in place and it will be helpful in determining a strategy for the information security program.

Refer to the *Asset Protection* section in this Guide for details.

Step 3 – Identify all relevant laws, regulations, statutes, and statewide policies applicable to the agency

Depending upon the agency's business, there may be laws and regulations that may apply to the way certain types of information are managed. Two common ones that may be applicable include the Health Insurance Portability and Accountability Act (HIPAA) requirements if the agency manages certain types of health information and Payment Card Industry (PCI) requirements if the agency accepts payment cards like Visa.

The SAM is a central point for statewide policies, procedures, regulations, and information. SAM Sections 5300-5399 directly relate to information security. Reviewing these requirements will assist in better understanding the responsibilities in complying with them.

Refer to the *Policy Management* and *Compliance* sections in this Guide for details.

Step 4 – Understand the agency's program areas and business needs

Meet program managers and staff to improve personal relations and better understand the business needs of the program areas, if it is not already well understood. Identify and document the following criteria:

- *Identify the size of the agency to better determine the intensity of the risk management process needed*. Typically, small agencies have 100 or few employees, medium agencies have between 101 and 1500 employees, and large agencies have more than 1501 employees.

- *Determine the complexity of the agency's program structure.* The more complex the program structure, the more it directly impacts the interdependencies and functional relationships that must be managed effectively for an agency to sustain an acceptable level of security. Typically:

  - Agencies with one or two programs have low complexity.
  - Agencies with three to seven programs have medium complexity.
  - Agencies with eight or more programs have high complexity.

- *Determine the significance of privacy and confidentiality issues within the agency*. The degree that privacy and confidentiality requirements impact an agency has a significant impact on how information security risks must be managed. Agencies that oversee health or medical related information, law enforcement systems, or Supervisory Control and Data Acquisition (SCADA) systems, for example, may determine that information security risks must be managed with an increased focus on higher levels of mitigation strategies, than an agency that doesn't manage those types of systems. Typically:

  - Agencies with privacy and confidentiality issues in only their administrative program are low impact.
  - Agencies with one or two additional programs with privacy or confidentiality issues are medium impact.
  - Agencies with three or more programs with privacy or confidentiality issues are high impact.

- *Determine how reliant the agency is on technology*. Almost all agencies rely on technology for service delivery and business process support. Some agencies deliver critical services for the state.

  - Agencies that rely on technology for only administrative processes or programs have a low reliance on technology.
  - Agencies with two or fewer programs that rely on technology have a medium reliance on technology.
  - Agencies with three or more programs or even one "critical to the state" program have a high reliance on technology.

- *Determine if the agency or a contractor (outsourced) manages the agency's technology infrastructure.* The number and degree of dependencies involved in managing the technology infrastructure used to deliver production services that support the business of the agency is a significant element of the risk management equation for the agency. The reliance on outsourced contractors, such as Internet Service Providers, Application Service Providers, email providers, Web hosting services, network service providers, IT business partners, and storage and e-discovery services, require contracts and service level agreements and the resulting interdependencies all impact information security risks that must be managed effectively for the agency to succeed. Typically:

  - Agencies with a technology infrastructure with two or fewer service providers have a low level of dependency complexity.
  - Agencies with three to five service providers have a medium level of dependency complexity.
  - Agencies with more than five service providers have a high level of dependency complexity.

- *Determine the maturity of the agency's operational processes.* Process maturity can be measured in terms of how successful the existing processes are used to operate the systems and IT resources that support the agency's business programs. Some elements to consider include:

  - How effectively production incidents and problems are resolved
  - How well changes are introduced into the production environment
  - How well production processes are documented
  - How effective the backup and recovery processes work
  - The depth of IT support in the agency

- How effectively requests for change are managed
- How effectively capacity requirements are planned for
- How well high availability requirements are managed, and
- How effectively security vulnerabilities are managed

This area can be difficult to assess if information about production problems and operational issues are only known to a limited number of staff, so it may be necessary to work with the agency's Chief Information Officer (CIO) or the IT operations manager. Typically:

- Agencies with a low level of maturity spend most of their IT operations time fixing problems or redoing work that was incorrect when first attempted. Process change is slow and documentation is not often available.
- Agencies with a medium level of maturity are able to schedule and implement simple system changes on schedule. They utilize repeatable documented operational processes. They are able to plan for changing system requirements and implement changes before they become emergencies.
- Agencies with a high level of maturity track and manage their performance on resolving incidents and problems. All areas of IT support use structured operational processes to control changes in the production environment. High availability configurations are included in the technology infrastructure and are effectively monitored and managed.

Step 5 – Determine an acceptable level of risk

Using the results from Step 4, enter the criteria values in the following table. Add the scores vertically and enter them into the Assessment Score row. Add all the assessment scores to get the Recommended Strategy Score.

Risk Management Strategy Criteria	Small or Low (5)	Medium (10)	Large or High (20)	N/A (0)
Determine the size of the agency to better determine the intensity of the risk management process needed.				
Determine the complexity of the agency's program structure.				
Determine the significance of privacy and confidentiality issues within the agency.				
Determine how reliant the agency is on technology.				
Determine if the agency or a contractor (outsourced) manages the agency's technology infrastructure.				
Determine the maturity of the agency's operational processes.				
Assessment Scores				
Recommended Strategy Score				

Step 6 – Choose an appropriate risk assessment tool

Using the Recommended Strategy Score obtained in Step 6, an agency can more appropriately choose a risk assessment tool that will determine gaps, risks and requirements based upon the agency's business needs. The resulting information from the assessment can then be analyzed to determine what level of controls to put into place. The Risk Assessment Toolkit can assist agencies in choosing an appropriate risk assessment tool and is available on the OISPP's Web site at www.infosecurity.ca.gov/. The tools identified below are described in more detail on the Web site.

- Agencies with a Recommended Strategy Score under 50 can probably begin with the basic *Information Security Risk Assessment Checklist*.
- Agencies with scores between 51 and 75 can begin with an *Assessment Tool for State Agencies*.
- Agencies with scores above 76 should consider using the *Assessment Tool for State Agencies* and supplement the process with the *SANS Information Security Management Audit Checklist* to more effectively manage the greater risk management complexity present in the agency. The other tools cited in the "Advanced" section on the Risk Assessment Toolkit Web page are informational and may contain useful components for the most complex risk management issues facing an agency.

A fundamental management responsibility is to provide for adequate security of information and the systems that process it. Understanding the current status of the information systems and controls provides the ability to make informed decisions and appropriately mitigate risks to an acceptable level.

A self-assessment provides an agency with a method to determine the current status and, where necessary, establish a target for improvement. The typical self-assessment guide utilizes an extensive questionnaire containing defined control objectives and techniques against which a system can be tested and measured. A review does not necessarily establish new security requirements. The control objectives and techniques come directly from long-standing requirements found in statute, policy, and guidance on security. Not only are gaps identified, but there is an opportunity to see where progress is being made; sometimes significant progress that may not be visible to the agency.[1]

See the *Risk Management* section in this Guide for more details.

Step 7 – Develop a work plan

The results of the assessment conducted in Step 6 must be documented to organize the most critical risks and resulting initiatives to mitigate or remediate them, track the progress, and identify anticipated completion dates. Developing a work plan and schedule, and keeping it up-to-date, will assist in managing the information security program effectively. From this work plan, the ISO can provide routine progress reports to the governance committee and executive management to keep them apprised of progress and issues.

[1] County of Sacramento, "Anchor County of Sacramento, "Anchor Your Information Security Program" Booklet by Jim Reiner.

Step 8 – Measure the progress against the previously established baseline

Over time, it is important to measure progress and to articulate successes in the improvement of an agency's information security program. Likewise, if an area is not improving as expected, this measurement can prompt adequate steps to get it back on track. Measure against the baseline established during Step 2.

Step 9 – Begin to manage risk through incremental changes

As the information security program matures, it will be easier to manage risk through incremental changes, rather than attempting to collect all new information and review the entire risk management process. For example, as a new system is implemented, or there is a change to the network infrastructure, an assessment of these particular areas may be appropriate.

SAM Section 5305.1 requires agencies to carry out the risk analysis process "…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."

Refer to SAM Sections 5305 through 5305.2 for details regarding policy.

This suggested implementation strategy and approach is an effective way to determine how to most effectively perform a Risk Assessment and strengthen an agency's risk management plan.

Security Components

Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for any agency to successfully implement and maintain an acceptable level of security.

A successful risk management program is more than a simple checklist of do's and don'ts, and a few policies and procedures. It is a proactive, ongoing program of identifying and assessing risk, and weighing business tradeoffs on acceptable levels of risk against ever changing technologies and solutions.

Risk management is a well understood and fully documented discipline. A risk management discipline, like the National Institute of Standards and Technology (NIST) Risk Model, typically encompasses three processes: assessment, mitigation, and evaluation. But, it is important to note that effective risk management may also be two dimensional – process-oriented and relevancy-oriented.

- Process-oriented addresses whether the person(s) conducting a risk assessment has asked the right questions to assess risks adequately within the agency and he/she has an effective process to ensure conclusions reached in the risk assessment properly translate into a work plan that can be executed to achieve the needed results.
- Relevancy-oriented refers to the importance the person(s) conducting the risk assessment places on the risks identified to ensure they are relevant to the agency.

Risk assessment is the first process in risk management. Agencies should use risk assessment to determine the extent of the potential threat and the risk associated with an IT system or an operational function. Depending upon the complexity and criticality of an agency's business, the risk assessment process may encompasses up to nine primary steps, which include identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

The third process of risk management, evaluation, is ongoing and evolving. Evaluation emphasizes the good practice to develop an effective risk management program within the agency's information security program. Not only should the risk management program engage changes to existing systems, but should also integrate into the agency's operational functions, as well as the System Development Life Cycle (SDLC) for new systems and applications.

Refer to "*A Suggested Implementation Strategy*" section in this Guide for a recommended strategy for implementing an effective information security program.

Best Practices

- Assign an individual, usually the ISO, to be responsible for leading risk assessment.
- Appoint a team of relevant business and IT personnel to participate in the risk assessment process.
- Through a comprehensive business impact analysis, identify the agency's information assets, then categorizes and prioritizes these assets based on classification and criticality.
- In the context of the agency's planning, acquisition, and change management processes, select and implement cost-effective protective measures.
- Document risk assessment results in a management report and submit it to the agency director.
- Document and preserve management decisions regarding the accepted level of risk.
- Develop a work plan to address the most critical risks and track their progress toward remediation.

Refer to SAM Section 5305.1 for details regarding policy.

Important Resources

- Risk Assessment Toolkit – www.infosecurity.ca.gov/
- NIST Risk Management Program – www.csrc.nist.gov/
- ISO 27002 – Risk Assessment and Treatment

Policy Management

Policy Management refers to the practices and methods used to create and maintain security policies to translate, clarify, and communicate management's position on high-level security principles. Policy management includes development, deployment, communication, updating, and enforcement of agency security policies. A successful policy must be independent of specific hardware and software decisions to adapt to changes in an agency's business environment.

To be practical and effective, specific policies must be applied to an agency's environmental and operational business and supported through standards, guidelines, processes, and procedures. A suggested policy framework might include:

High-Level Organizational Policy	**Standards, Guidelines, Processes and Procedures that Support the Policy**
Asset Protection	Data classification, access control, personnel practices, change management, network security and disaster recovery
Vulnerability	Change management, wireless, vulnerability testing, application development
Threats	Incident management, penetration testing, audits, firewalls, malware prevention
Awareness	User education, IT education, annual certification, administrative rules
Appropriate Use	Education, Web filtering, content filtering, peer-to-peer, resource use for personal purposes (i.e., instant messaging, email, remote access, Internet, etc.)

Best Practices

- Develop a formal approval process and identify individuals and roles for approval of new policies and changes to existing ones. (Refer to the "Organizing Information Security" section in this Guide for details.)
- Clearly identify security policy-related processes, including what activities are to be performed, their frequency, and the position that is responsible to perform the process.
- Ensure policies, standards, and guidelines address legislative, regulatory, and contractual requirements.
- Establish policies and standards that clearly identify what can and cannot be performed, stored, accessed and used through the organization's computing resources (e.g., acceptable use policy, peer-to-peer policy, Internet use policy).
- Review policies periodically or when there have been changes in internal processes, laws or regulations, standards, or any changes to related policies, including the implementation of news systems or applications.
- Once security policies and procedures have been established, disseminate to all appropriate users, staff, management, and third party providers.
- Enforce policies through automated means where technically feasible.

- Obtain and maintain an established record of acknowledgement that all appropriate users, staff, management, and third party providers have read the policies and understand the consequences of non-compliance with the policies.

Important Resources

- SAM Information Security Sections 5300-5399 – www.sam.dgs.ca.gov/TOC
- SP 800-100 Information Security Handbook for Managers – www.csrc.nist.gov/publications/nistpubs/
- The SANS Security Policy Project – www.sans.org/resources/policies/#template
- ISO/IEC 27002 – Security Policy
- Appendix B: Acceptable Use Security Policy Sample, found in the back of this Guide

Organizing Information Security

A governance structure is essential to organizing information security within and across the organization. Governance maintains balance between the value of information security, the management of security-related risks, and increased requirements for control over information. Value, risk, and control constitute the core of an effective information security governance structure.

Information security governance is the responsibility of senior management and executive staff. Typically an agency's ISO will lead, or be highly participative in the governance of the information security program. It consists of the leadership, organizational structures, and processes that ensure the agency's information security program sustains and extends the agency's strategies and objectives in accordance with business requirements and relevant laws and regulations. Information security is a top-down process requiring a comprehensive security strategy that is explicitly linked to the agency's business processes and strategy. Security should address the entire organizational processes, both physical and technical, from end to end. The tone at the top should be conducive to effective security functionality. It is unreasonable to expect lower-level personnel to abide by security policies if senior management does not.

Information security governance generates significant benefits, including:

- A structure and framework to optimize allocation of limited security resources.
- Reducing operational costs by providing predictable outcomes and mitigating risk factors that may interrupt the business process.
- Achieving consensus in the organization by balancing the needs of its business against information security requirements and maximizing the value of information security resources.
- Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels.
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care.
- Assurance of effective information security policy and policy compliance.
- Improving trust in customer relationships and protecting the organization's reputation.

Additionally, information security must be part of the agency's core business functions. It involves strategically planning an ongoing effort to adopt security as an enabler to the agency's business through the implementation of an information security program. It must be structured around the policy and measurement (metrics) role rather than solely based as an operational function. Designating an individual to fulfill the role of ISO, who is directly responsible to the agency director (SAM Section 5315.1), and who possesses the professional qualifications, including the training and experience required to administer an information security program is crucial to its success. See the OISPP's *The Guide for the Roles and Responsibilities of an Information Security Officer Within State Government* for details regarding an ISO's role and responsibilities.

Best Practices

- Management should actively and visibly support information security throughout the organization.
- Establish other assignments of specific roles and responsibilities for information security and promote cooperation and collaboration among these individuals across the organization (e.g., ISO, CIO, legal, human resources, management, system developers, system administrators, end-users).
- The ISO should regularly report to management on the program's adequacy and effectiveness.
- Regularly review investment in information security to ensure continued alignment with the agency's business program strategies and objectives.
- Establish confidentiality or non-disclosure agreements with third parties to protect confidential information using legally enforceable terms.
- Implement an independent review of information security at planned intervals to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security.
- Consider implementing service level or operating level agreements with customers and program areas to document an agreed-to level of expected service, especially for information technology services.

Important Resources

- "*A Suggested Implementation Strategy*" section found on page 5 of this Guide.
- *The Guide for the Roles and Responsibilities of an Information Security Officer Within State Government* – www.infosecurity.ca.gov/
- Office of State Audits and Evaluations – www.dof.ca.gov/FISA/OSAE/OSAE.asp
- NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook www.csrc.nist.gov/publications/nistpubs/
- ISO/IEC 27002 – Organization of Information Security

Asset Protection

Asset Protection refers to a process where agencies identify and inventory assets, agree upon ownership and the classification of information, and document the process of safeguarding each asset to protect against loss or theft. Inventories of assets can assist to ensure effective asset protection occurs, identification of missing assets, and may satisfy other business purposes, such as health and safety or other asset management requirements. An agency must know what its assets are in order to identify what is missing. Compiling an inventory of assets is the first step towards risk management of agency assets.

Agencies must ensure the necessary policies, standards, guidelines, processes, and procedures are in place to be in compliance with laws, regulations, statutes, and state policies with respect to asset inventory, identification, classification, use, and disposition requirements. This effort may involve establishing cooperative relationships with management in other functional units across the organization (e.g., business areas, human resources and labor relations, business services, procurement, IT services, and legal).

Policies are basic foundations; however, agencies must also ensure that all information created and used by its employees and contractors are properly classified. Classification categorizes information, whether that information is contained on paper or in electronic format, in terms of its sensitivity to loss, disclosure, and availability. The classification is required to implement the appropriate security controls. Data classification is the responsibility of the data owner, or their designee, and requires the initial classification, as well as periodic reviews, to ensure the appropriate level of security controls are in place. There are many types of assets that require protection, including, but not limited to:

- Information – databases and files, contracts and agreements, system documentation, training material, business continuity plans, specialized contact lists, audit trails, and operation or support procedures.
- Software assets – application and system software, development tools, and utilities.
- Physical assets – computer equipment, communications equipment, uninterruptible power supplies, removable media, Closed Circuit Television (CCTV), and identification badges.
- Services – computing and communications services and general utilities, such as telephone, internet access, heating, lighting, and power and air conditioning.
- Intangibles such as reputation and image of the organization.

Best Practices

- Classify the agency's information in terms of its value, legal requirements, sensitivity, and criticality.
- Implement policy and guidance to ensure employees and contractors have been informed of their responsibility for asset protection. This may include tracking of assigned equipment through signed equipment checkout forms, and maintenance of signed security acknowledgement forms.
- Implement policy and guidance to ensure the agency enforces the policy in a consistent and fair manner when policy violations occur. This responsibility may involve assisting management with the development of corrective action plans and memoranda.

- Review and validate the establishment and effectiveness of asset management policies, procedures and practices through observation, reviews, interviews, and periodic tests of safeguards.

Important Resources

- Department of General Services – SAM – www.sam.dgs.ca.gov/TOC/default.htm
- State Records Management Act (Government Code Sections 14740-14770)
- Common Risks Impeding the Adequate Protection of Government Information – www.csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf
- ISO/IEC 27002 – Asset Management

Human Resources Security

Human Resource (personnel) Security refers to those practices, technologies, and services to ensure the employees and contractors authorized to access or maintain systems have the appropriate levels of access needed to perform their duties. Because of their internal access levels, authorized users pose a potential threat to systems and data. Additionally, reducing the amount of users with system administrator privileges reduces the risk of accidental damage or loss of information and systems.

A key component to assure that legitimate users understand their role and responsibility for information security is through an ongoing awareness program. An effective program ensures employees and contractors know about information security and privacy relative to their job responsibilities. A good awareness program essentially markets the agency's existing policies, standards, and practices.

A successful security awareness program should target various groups (such as employees and contractors, IT staff, or managers and supervisors) with information pertinent to their respective roles. Most users would be interested in awareness material addressing Internet use, email, and handling confidential information. Technical support personnel would be more focused on access control, anti-virus, and patch management administration. The executives would be more interested in the benefits of enabling business through information security, risk management, and business continuity.

As outlined in the SAM Section 5300.3, each state agency is required to provide annual security and privacy training to all employees and contractors.

Best Practices

- Provide for separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
- Remove physical and logical access as soon as an employee or contractor leaves, retires, or is terminated.
- Create forms and instructions to ensure return of state property and notification to appropriate internal staff for employee transfers and terminations.
- Provide specific requirements regarding use and access for non-state entities (including vendors and contractors) and document in agreements in order to comply with all state policy and law regarding use of information resources and data. (SAM Section 5305 and 5310)
- Implement formal disciplinary processes for employees who have committed a security breach.
- Promote security awareness using techniques such as: posters, email messages, formal instruction, web-based instruction, videos, newsletters, and security awareness days.
- Ensure all users sign confidential and acceptable use statements (SAM Section 5310) annually.
- Train all users to quickly identify threats, and how to respond to security incidents.
- Inform all users about agency policies and procedures.
- Regularly review and update training content to reflect changes to the agency's environment.

Important Resources

- Department of Personnel Administration – www.dpa.ca.gov/
- Office of Information Security and Privacy Protection – www.oispp.ca.gov/
- California Office of HIPAA Implementation – www.calohi.ca.gov/
- NIST SP 800-50 – Building an Information Technology Security Awareness and Training Program – www.csrc.nist.gov/publications/nistpubs/
- ISO/IEC 27002 – Human Resources Security

Physical and Environmental Security

Physical and Environmental Security refers to those practices, technologies and services used to address the threats, vulnerabilities, and counter measures utilized to protect information assets and the premises in which they reside. These safeguards take into account: 1) the physical facility housing the information resources; 2) the general operating location and environmental factors; and 3) any additional facilities that support the operation of the information systems (e.g., server room/closet, data centers). They may be situational depending upon building and leasing requirements.

Best practices can be separated into four categories:

1. *Authorization* ensures that entry into an organization's facilities and restricted areas is done so with proper authorization.
2. *Access control* ensures that entry into facilities is controlled and limited to personnel with proper authorization and credentials.
3. *Monitoring* ensures that entry into an organization's facilities is monitored for breaches and/or compromises.
4. *Logging* ensures that entry and access to facilities and data centers is logged for audit purposes.

Best Practices

- Locate system components used to deliver *mission critical*, confidential, or sensitive programs in a strategically placed location with limited access, and ensure it is an environmentally controlled area. The placement might include an access that is restricted, windowless, temperature controlled area, with special floors, fire protection, Heating, Ventilation, Air Conditioning and Cooling (HVAC), UPS, and walls extending through the ceilings.
- Control access to *mission critical* and *non-mission critical* computer hardware, wiring, displays and network by the principle of least privilege (e.g., assigned the fewest privileges consistent with their assigned duties and functions).
- Document system configurations (such as hardware, wiring, displays, and network) and treat it as sensitive information. Any changes should be governed by a formal change management process.
- Ensure physical access security for back-up systems, tapes, and storage media meet or exceed physical access security of the primary facilities and related access controls.
- Monitor and audit access to facilities, computer hardware, wiring, displays, and networks (e.g., badges, cameras, access logs, sign-in sheets, etc.).
- Establish additional controls (such as CCTV or cameras) and special access authorizations for restricted areas (such as network area, computer rooms, or any area processing financial implements, such as cash or checks).
- Include contractual language for physical security services (e.g., security guards) by requiring full security clearances for all physical security personnel. The clearances should be completed prior to the security guards reporting to the facility.
- Ensure that security guards check credentials of those entering facilities.
- Establish physical security policies, standards, and guidelines and communicate them to all personnel, including employees, contractors, vendors, and volunteers.
- Establish processes to ensure physical security logs are reviewed and retained according to established policy.

- Implement physical and software controls for information assets such as, but not limited to, locked file cabinets for paper records containing personal and confidential data, and locking cables, passwords, and encryption for computing assets.
- Develop, maintain, and regularly review a master list of access authorizations for each person and facility within an organization's infrastructure.
- Promptly deactivate badges and access codes when an employee, contractor, vendor, or volunteer leaves, retires, or is terminated.
- Regularly test and audit monitoring devices, back up power, and access controls to ensure they are functioning properly.

Important Resources

- SP 800-12 – An Introduction to Computer Security: The NIST Handbook – www.csrc.nist.gov/publications/nistpubs/
- ISO/IEC 27002 – Physical and Environment Security

Communications and Operations Management

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it.

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code. Although the elements are described in terms of the technologies needed and/or used for system and communication protection it is really the *processes* that administer and monitor the technologies that assure the required level of security.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities. As always, it is a balance of these types of controls against business requirements, cost, efficiency, and effectiveness.

Operations management covers IT assets throughout their lifecycle. Thus, it is greater than the cost of just purchasing assets, and includes all ongoing maintenance, security, monitoring, and problem resolution. The overall goal of operations management is to lower the total cost of ownership of all organizational devices, from enterprise servers to mobile devices attached to the network, while keeping the environment secure.

Proper operations management safeguards all of the organization's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers. The method of protection used should not make working within the agency's computing environment an onerous task, nor should it be so flexible that it cannot adequately control excesses. Ideally, it should obtain a balance between these extremes, as dictated by the agency's specific business needs.

This balance depends, at least in part, on two items. One is the value of the data, which may be stated in terms of intrinsic value or monetary value. Intrinsic value is determined by the information's criticality and sensitivity – for example, health- and personal-related information may have a high intrinsic value. The monetary value is the potential financial or physical losses that would occur should the information be breached or violated. The second item is the ongoing business need for the information, which is particularly relevant when continuous availability (i.e., round-the-clock processing) is required.

Best Practices

- Implement cryptographic (encryption) solutions when the confidentiality or sensitivity of information must be maintained while a message is in transit between computing devices and when confidential or sensitive information is stored in a file or database.
- Deploy and routinely update appropriate anti-virus, anti-spyware, and file extension blocking solutions at the gateway entry points and on the desktop and server systems to prevent these systems from being compromised.
- Ensure a firewall or other boundary protection mechanism is in place and has the ability

to evaluate (1) source and destination network addresses, and (2) determine the validity of the service requested.

- Deploy appropriate Intrusion Detection System and Intrusion Prevention System (IDS/IPS) solutions at the correct network location(s) and monitor to detect when the agency is under attack so an effective detection and defense strategy can be deployed.
- Implement an appropriate change management process to ensure changes to systems are controlled.
- Provide for separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
- Establish procedures to implement an agreed backup policy and strategy, including the extent (e.g., full or differential/incremental), frequency, offsite storage, testing, physical and environmental protection, restoration, and encryption.
- Secure certain internal data and systems (Accounting and Human Resources, for instance) from other data and systems on the networks.
- Do not place confidential or sensitive data on any application servers, database servers, or infrastructure components that require direct Internet access in the Demilitarized Zone (DMZ). Components that meet these criteria must be placed behind the DMZ where they are not accessible from the Internet and can only interact with DMZ components through a second and more restrictive firewall.
- Establish appropriate procedures to protect documents, computer media, information/data, and system documentation from unauthorized disclosure, modification, removal, and destruction, including suitable measures to properly dispose of media when it is no longer needed.
- Establish procedures and standards to protect information and physical media containing information in transit, including using facsimile machines, exchange agreements between the agency and external parties, transportation of physical media, and monitoring (e.g., audit logging, monitoring system use).
- Implement appropriate levels of security monitoring including intrusion detection, penetration testing, and violation analysis.
- Perform reviews of audit trails on a regular basis to alert an agency to inappropriate practices.
- Ensure preventive or detection controls are in place to decrease or identify the threat of unintentional errors or unauthorized users accessing the system and modifying data.
- Implement appropriate retention policies as dictated by the agency's policies, standards, legal and business rules.
- Implement appropriate documentation such as security policies and procedures, business contingency plans, disaster recovery plans, and incident response plans, including a plan for cyber attacks, such as a denial of service attack.

Important Resources

- All NIST Guidelines below are available at www.csrc.nist.gov/publications/nistpubs/:
  - NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook
  - NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
  - NIST SP 800-45 Guidelines for Electronic Mail Security
  - NIST SP 800-83 Guide to Malware Incident Prevention and Handling
  - NIST SP 800-88 Media Sanitization Guide
- Department of General Services Records Management Program – www.osp.dgs.ca.gov/recs/default.htm
- ISO/IEC 27002 – Communications and Operations Management

Access Control

Access Control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of the agency's information assets. Key components include identification, authentication, and authorization. These components apply to people, process, and technology devices.

Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about the levels of access that should be given. The key feature of an identity process is that each member of the agency, and any other entity about which access decisions need to be made, is uniquely identifiable from all other members.

The authentication process determines whether someone or something is, in fact, who or what it is declared to be. Authentication validates the identity of the person or technology device. Typical authentication methods include passwords, fixed IP addresses, security tokens, smart cards, biometrics, and secret information known only to the person. Authentication factors can be something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometric). Two-factor authentication consists of two of the three factors (e.g., password and token) in these distinct categories. For the purpose of access control, authentication verifies one's identity through IT.

Authorization is the process used to grant permissions to authenticated users. Authorization grants the person(s), through technology or process, the right to use the information asset(s). Examples of the authorization process include signed access control forms for new employees, signed contracts between entities granting information rights, or assignment to a specific group or role. The access rights to the information are then programmed or entered into the security system via an access list, directory entry, or view tables, for example, so the authorization rules can be enforced.

Best Practices

- Establish formal procedures for the owners, or owner designee, of the data to authorize access to information systems and services that use their data.
- Audit access level rights at regular intervals.
- Monitor and audit system access and use.
- Ensure the security system can identify and verify the identification and, if necessary, the location of each authorized user.
- Apply access method of "least privilege" where access to, or the flow of information, is only granted to the extent necessary to get the job done.
- Authenticate individuals and technology components consistent with acceptable risk levels determined by the information owners.
- Use logon banners to display a general security notice and acceptance of use conditions.
- Remove access upon employee termination or when the need no longer exists.
- Establish password standards such as minimum length requirements with a combination of characters and numbers, and appropriate periodic password aging.
- Restrict connection time to appropriate business hours.
- Initiate automatic logout or protected screen savers by the system after a specific period of inactivity.

Important Resources

- Sample Banner Language – www.infosecurity.ca.gov/
- NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook www.csrc.nist.gov/publications/nistpubs/
- NIST SP 800-100 Information Security Handbook for Managers: www.csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- ISO/IEC 27002 – Access Control

Information Systems Acquisition, Development, and Maintenance

Agencies should ensure that security is an integral part of information systems, which include operating systems, infrastructure, applications and off-the-shelf products, services, and user-developed applications. Security requirements should be identified and agreed upon prior to the development and/or implementation of information systems and documented as part of the overall business case. The requirements must also ensure compliance with any applicable laws, regulations, statutes, and state policies are met (e.g., HIPAA, PCI Standards, and SAM). Security should be considered and designed in from the beginning and during the entire system development lifecycle; not bolted on afterwards.

Best Practices

- Implement requirements for ensuring authenticity and protecting message integrity in applications.
- Implement the use of cryptographic (encryption) measures to protect confidential or sensitive information and protect encryption keys from modification, loss, and destruction.
- Implement input and output data validation checks to ensure data is correct and appropriate.
- Implement processes to control the installation of software on operating systems.
- Implement procedures to select, protect, and control test data. Do not use test data in a production environment or use production data in a test environment without careful consideration.
- Limit access to program source code and place source code in a secure environment.
- Implement change control procedures to minimize the corruption of information systems.
- Technical review of applications after operating system changes should occur to ensure there is no adverse impact on operations or security.
- Limit modifications to vendor-supplied software packages.
- When outsourcing software development, consider contractual language for licensing arrangements, code ownership, quality and security functionality, testing to detect malicious code, and escrow arrangements in the event of third party failure.
- Establish an effective management process for technical vulnerabilities, such as assessment of patches before implementation, action to be taken to correct vulnerabilities, and timelines for correcting vulnerabilities.

Important Resources

- U. S. Department of Homeland Security – Build Security In – https://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- California Office of the State Chief Information Officer – www.cio.ca.gov/
- The following NIST Guidelines are available at: www.csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
  - NIST SP 800-55 Security Metrics Guide for Information Technology Systems
  - NIST SP 800-44 Guidelines for Securing Public Web Servers
- ISO/IEC 27002 – Information Systems Acquisition, Development and Maintenance

Information Security Incident Management

Information Security Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. Development, documentation, and implementation of an information security incident response plan provides the framework for an agency to proactively manage incidents when they occur. Typically, the main point of contact is the agency's ISO. To ensure the contact is always available, a backup should be identified and trained on the processes and procedures of incident management.

It is important that those responsible for incident management understand the criteria for notification and reporting of information security incidents. Effectively, the criteria for an incident includes the theft, loss, damage, unauthorized destruction, unauthorized modifications, or unintentional or inappropriate release of any data classified as confidential, sensitive, or personal of state assets. Upon the discovery of any incident that meets the defined criteria in SAM Section 5350.2, agencies are required to report information security incidents immediately upon discovery. The notification and reporting criteria covers the following five categories: State Data (includes electronic, paper, or any other medium), Equipment, Inappropriate Use and Unauthorized Access, Computer Crime, or any other incident that violates agency policy. Quick notification and response to an incident is essential to reduce the impact to the agency by implementing the appropriate safeguards so there is no further damage. For example, if a virus infects a system, removing that system from the network as quickly as possible is essential so the virus does not spread.

Tracking incidents provides the ability to observe trends and anomalies and ensures that corrective actions implemented continue to provide the appropriate safeguards. Tracking also includes the documentation from a prompt investigation of an incident. The investigation is conducted to determine the facts of the incident: what happened, how it happened, when it happened, why it happened, who it happened to. From the facts collected, mitigation strategies are determined to eliminate or greatly reduce the incident from reoccurring. Additionally, the information collected is important because California law requires breach notifications to be sent to impacted individuals when specific personal information is lost, stolen, or disclosed. To ensure appropriate steps are taken, agencies should establish procedures for addressing notice-triggering disclosures, through discussions with the privacy officer and legal office.

Finally, providing awareness and training to employees through the agency's annual security and privacy awareness training will be a continuing reminder of the internal procedures and processes for identifying and reporting an incident. After all, the employees are the first line of defense. Make sure they know who to call, when to call, and that the person being called is available and responsive.

Best Practices

- Ensure all employees, contractors, and third party users know how to identify an incident, when it should be reported, and to whom it should be reported to.
- Implement procedures to establish an effective and orderly response to security incidents.
- Establish internal procedures for the collection and protection of evidence in disciplinary action or criminal situations.
- Establish an internal process for the reporting of incidents to external entities.

- Establish an internal process for reporting disclosure incidents to privacy officers, legal office, and others within the department that would be included in the notification process.
- Corrective action resulting from previous incidents should be applied to limit recurring or high impact incidents from happening again.
- Implement recovery procedures to ensure the agency has the ability to re-establish business should equipment (e.g., server) and its related systems and information is unavailable during an investigation.
- Include the identification of incidents and reporting process in the annual security and privacy awareness training.

Important Resources

- Office of Information Security and Privacy Protection – www.oispp.ca.gov/
- California Highway Patrol – www.chp.ca.gov/
- California Department of HIPAA Implementation – www.calohi.ca.gov/
- The following NIST Guidelines are available at: www.csrc.nist.gov/publications/nistpubs/
    - SP 800-61 NIST Computer Security Incident Handling Guide
    - NIST Computer Forensics Guidance (November 2001)
- ISO/IEC 27002 – Information Security Incident Management

Disaster Recovery Management

State agencies must ensure that a disaster recovery plan (also referred to as an operational recovery plan) is in place and routinely tested. The purpose of this plan is to provide for the continued IT support of critical business functions by developing a recovery strategy and procedures that ensures timely resumption of essential IT operations, the recovery of critical applications and information, and the delivery of the services to the workforce and customers. Creation, maintenance, and annual testing of a plan will minimize the impact of recovery and loss of information assets from events from a single disruption of business to a disaster. Planning and testing provides a foundation for a systematic and orderly resumption of all computing services within an agency when disaster strikes.

An active disaster recovery management process will minimize the consequences of damages from a disruption and ensure that the information and systems required for an agency's critical business processes are available in the time frame needed. Effective plans require the participation of the staff in both the business and IT areas. Conducting a Business Impact Analysis (BIA) will aid in the identification of consequences of disasters, security failures, loss of service, service availability, the prioritization of critical business processes and the time frame that the processes must be made available to meet the mission of the agency. Validation that the plan will meet the recovery needs of the agency is made through testing of the plan. And, training of the staff responsible for recovery will ensure their readiness in their role during a recovery phase.

As required in SAM Section 5355 -5355.3, all state agencies are required to conduct operational recovery planning and develop, maintain, and test a disaster (operational) recovery plan. The disaster recovery plan must also support and align with the agency's Continuity of Operations (COOP) and Continuity of Government (COG) efforts.

Best Practices

- Conduct business impact analysis to determine critical business functions, assets involved in critical business processes, and identify critical business systems.
- Document a plan to maintain, restore, and recover operations to ensure availability of information at the required level and time frame following a disruption, failure of critical systems, or disaster.
- Identify key team members to ensure they are aware of the plan and their responsibility and role in the recovery process.
- Training key team members to ensure the recovery procedures are appropriate, current, and accurate.
- Test and regularly update the plan. Use a variety of testing techniques, such as tabletop exercises, simulations, backup capabilities, and tests of suppliers and services.

Important Resources

- Office of Information Security and Privacy Protection – www.infosecurity.ca.gov/
- Office of Emergency Services – www.oes.ca.gov/
- Disaster Recovery Institute – www.drii.org/
- ISO/IEC 27002 – Business Continuity Management

Compliance

Compliance refers to the process framework for ensuring conformity to applicable federal and state statutory, regulatory, and contractual requirements and verifying adherence to statewide reporting requirements. There are two major pieces to the Compliance component: internal and external compliance.

Internal Compliance:
Agencies should implement internal procedures to ensure compliance requirements are met, organizational records are protected, and controls are in place.

Best Practices

- Measure the success of the agency's information security program through metrics.
- Ensure the information security program governance structure provides the authority, leadership and guidance necessary to implement decisions and hold applicable parties accountable.
- Determine and implement corrective action plans for non-compliance.
- Ensure incident response and reporting is accurate, documented, and after action items are addressed.
- Ensure the information security program work plan is updated annually and tasks are executed as planned.
- Acquire software through known and reputable sources to ensure that copyright is not violated.
- Maintain proof and evidence of ownership of licenses, master disks, and manuals.
- Provide procedures for maintaining appropriate license conditions and disposing or transferring of software to others.
- Develop a retention schedule for identifying records and the period of time for them to be retained.
- Implement appropriate controls to protect records and information from loss, destruction, and falsification.
- Implement controls to safeguard systems during audits (e.g., limit to read only, produce a reference trail).

External Compliance:

- **Laws, Regulations, Statutes**
  Agencies must adhere to all applicable laws, regulations, and statutes, including but not limited to:

  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Civil Code Section 1798 et al (Information Practices Act of 1977)
  - California Government Codes, such as 11019.9 (enact and maintain a permanent privacy policy) and 6250-6270 (California Public Records Act)
  - Payment Card Industry Data Security Standards
  - California Financial Integrity and State Manager's Accountability Act
  - Family Educational Rights and Privacy Act (FERPA)

- **State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) Requirements**
  State agencies must adhere to all of the policy requirements outlined in SAM. The following required policy is set forth by the OISPP in SAM Section 5360 and 5360.1, to reduce the risk of misuse, disruption, or loss of state agency information assets. Agency heads are responsible for the oversight of their respective agency's information security program compliance and shall take reasonable measures to implement and report according to the following:

  - As noted in SAM Section 5355.1 and 5355.2, each agency must file an informational copy of its Operational Recovery Plan with the OISPP by the due date outlined in the Schedule for Submission of Operational Recovery Plans, found on the OISPP Web site at www.infosecurity.ca.gov/.
  - Agency management must promptly investigate and report suspected or verified incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and databases, as well as incidents involving loss, damage, or misuse of information assets to the California Highway Patrol immediately upon discovery. A report outlining the incident details, cost, and corrective action taken must follow within ten business days of reporting the incident. Details about this requirement can be found at www.infosecurity.ca.gov/incidents/.
  - By January 31 of each year, or as instructed by the OISPP, the director of each agency must certify that the agency is in compliance with state policy governing information technology risk management by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C).
  - By January 31 of each year, when changes occur, or as instructed by the OISPP, the director of each agency must provide contact information for the agency's ISO, the Operational Recovery Coordinator, their backups, and Privacy Coordinator on the form specified in SIMM Section 70A.

Important Resources

- Office of Information Security and Privacy Protection – www.oispp.ca.gov/
- Department of General Services (DGS) SAM – www.sam.dgs.ca.gov/default.htm
- Office of State Audits and Evaluation – www.dof.ca.gov/osae/overview
- California Department of HIPAA Implementation – www.calohi.ca.gov/
- NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule – www.csrc.nist.gov/publications/nistpubs/
- Payment Card Industry Data Security Standards – www.pcisecuritystandards. org/tech/
- ISO/IEC 27002 – Compliance

Appendix A: Security Policy Template

A security policy is the essential basis on which an effective and comprehensive security program can be developed. This critical component is the primary way in which the agency security plan is translated into specific, measurable, and testable goals and objectives. It is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within an agency.

The security policies developed must establish a consistent message of what is and what is not permitted with respect to an agency's information resources. Business objectives should drive the policy and it must align with the technical, legal, and regulatory environment of the agency. Additionally, policies must be supported by standards, guidelines, processes and procedures to be effective.

The following is a recommended outline of the components and characteristics for a security policy template. A sample Acceptable Use Policy using this outline is attached for reference as Appendix A.

Section 1 – Introduction:

A scope and purpose statement should be included in the introduction section. It should provide the reader with a brief description of what the policy states and why it is needed. The security stance of the agency should be identified.

Section 2 – Roles and Responsibilities:

It is important that the policy detail the specific responsibilities of each identifiable user population, including management, employees, and external parties.

Section 3 – Policy Directives:

The directive section of the policy should describe the specifics of the security policy. It should not dictate business objectives, but should broad, high-level, easy to understand, and support all legislation and regulation applicable. It should provide sufficient information to guide the development and implementation of supporting standards, guidelines, and procedures.

Section 4 – Enforcement, Auditing, Reporting:

This section should state what is considered a violation and identifies the penalties for non-compliance. The violation of a policy may imply or state disciplinary action which must be enforced.

Section 5 – References:

All references mentioned in the policy, including SAM requirements, legislative mandates and regulations, and applicable agency standards, guidelines and procedures should be identified.

Section 6 – Control and Maintenance:

This section identifies the author and owner of the policy. It describes the conditions and process in which the policy will be reviewed. A policy review should be performed on an annual basis to ensure that the policy remains current.

Appendix B: Acceptable Use Security Policy Sample

The following document is a sample Acceptable Use Security Policy using the outline identified in the Security Policy Template. The purpose of this sample document is to aid agencies in the development of their own policies by giving specific examples of what can be performed, stored, accessed, and used through the use of an agency's computing resources. It should be edited and modified to meet the agency's business needs and objectives.

As policy is developed, it must be thoroughly vetted through the agency's governance structure, or at a minimum the ISO, CIO, Legal Office, Equal Employment Opportunity Office, Human Resources, Labor Relations and any other unit within the agency as appropriate to ensure compliance with existing agency policies. Executive management approval and support is highly recommended and a key to its successful implementation. It should be noted that any policies that affect an employee's work environment must be vetted through the state unions. The agency's Labor Relations Office can provide guidance and assistance in that endeavor.

Refer to the *Human Resources* section in this Guide for guidance in informing employees about the release of new policies.

<AGENCY>
POLICY

INFORMATION SECURITY		**NUMBER:**	**xxxx**
		EFFECTIVE:	**mm/dd/yyyy**
		REVISED DATE:	**mm/dd/yyyy**
SUBJECT: ACCEPTABLE USE		**APPROVED:**	

SECTION 1 – INTRODUCTION

Information Resources are strategic assets of the <AGENCY> and must be treated and managed as valuable resources. <AGENCY> provides various computer resources to its employees for the purpose of assisting them in the performance of their job-related duties. State law permits minimal and incidental access to state resources for personal use. This policy clearly documents expectations for appropriate use of <AGENCY> assets. This Acceptable Use Policy, in conjunction with the corresponding standards, is established to achieve the following:

1. To establish appropriate and acceptable practices regarding the use of information resources.
2. To ensure compliance with applicable state law and other rules and regulations regarding the management of information resources.
3. To educate employees who may use these information resources with respect to their responsibilities.

This Acceptable Use Policy contains four policy directives. Part I – Acceptable Use Management Requirements, Part II – Ownership, Part III – Acceptable Use Requirements, and Part IV – Minimal and Incidental Use. Together, these Directives form the foundation of the <AGENCY> Acceptable Use Program.

SECTION 2 – ROLES AND RESPONSIBILITIES

1. <AGENCY> management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
2. <AGENCY> management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.
3. <AGENCY> Managers, in cooperation with the Security Management Division, are required to train employees on policy and document issues with policy compliance.
4. All <AGENCY> employees are required to read and acknowledge the reading of this policy.

SECTION 3 – POLICY DIRECTIVES

Part I – Acceptable Use Management Requirements

<AGENCY> will establish formal standards and processes to support the ongoing development and maintenance of the <AGENCY> Acceptable Use Policy.

The <AGENCY> Director and management will commit to the ongoing training and education of <AGENCY> staff responsible for the administration and/or maintenance and/or use of <AGENCY> information resources. At a minimum, skills to be included or advanced include user training and awareness.

<AGENCY>
POLICY

INFORMATION SECURITY

SUBJECT: ACCEPTABLE USE

NUMBER:	**xxxx**
EFFECTIVE:	**mm/dd/yyyy**
REVISED DATE:	**mm/dd/yyyy**
APPROVED:	

1. The <AGENCY> Director and management will use metrics to establish the need for additional education or awareness in order to facilitate the reduction in the threat and vulnerability profiles of <AGENCY> assets and information resources.
2. The <AGENCY> Director and managers will establish a formal review cycle for all acceptable use initiatives.
3. Any security issues discovered will be reported to the ISO, or designee, for follow-up investigation. Additional reporting requirements can be located within the Policy Enforcement, Auditing, and Reporting section of this policy.

Part II – Ownership

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of <AGENCY> are the property of <AGENCY> and employee use of these files is neither personal nor private. Authorized <AGENCY> information security employees may access all such files at any time without knowledge of the information resources user or owner. <AGENCY> management reserves the right to monitor and/or log all employee use of <AGENCY> information resources with or without prior notice.

Part III – Acceptable Use Requirements

1. Users must report any weaknesses in <AGENCY> computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
2. Users must report any incidents of possible misuse or violation of this Acceptable Use Policy through the use of documented misuse reporting processes associated with the Internet, Intranet, and email use standards.
3. Users must not attempt to access any data, documents, email correspondence, and programs contained on <AGENCY> systems for which they do not have authorization.
4. Systems administrators and authorized users must not divulge remote connection modem phone numbers or other access points to <AGENCY> computer resources to anyone without proper authorization.
5. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), security tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes.
6. Users must not make unauthorized copies of copyrighted or <AGENCY> owned software.
7. Users must not use non-standard shareware or freeware software without the appropriate <AGENCY> management approval.
8. Users must not purposely engage in activity that may harass, threaten, or abuse others or intentionally access, create, store, or transmit material which <AGENCY> may deem

to be offensive, indecent, or obscene, or that is illegal according to local, state, or federal law.

9. Users must not engage in activity that may degrade the performance of information resources; deprive an authorized user access to <AGENCY> resources; obtain extra resources beyond those allocated; or circumvent <AGENCY> computer security measures.
10. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of a <AGENCY> computer resource unless approved by <AGENCY>'s ISO.
 .
11. <AGENCY> information resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state, or federal law.
12. Access to the Internet from <AGENCY> owned, home based, computers must adhere to all the policies. Employees must not allow family members or other non-employees to access nonpublic accessible <AGENCY> computer systems.
13. Any security issues discovered will be reported to the ISO, or designee, for follow-up investigation. Additional reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.

Part IV – Minimal and Incidental Use
Government Code Section 8314 permits minimal and incidental personal use of state resources. At <AGENCY> this means:

1. Minimal and incidental personal use of email, Internet access, fax machines, printers, and copiers is restricted to <AGENCY> approved users only and does not include family members or others not affiliated with <AGENCY>.
2. Minimal and incidental use must not result in direct costs to <AGENCY>, cause legal action against, or cause embarrassment to <AGENCY>
3. Minimal and incidental use must not interfere with the normal performance of an employee's work duties.
4. Storage of personal email messages, voice messages, files, and documents within <AGENCY>'s computer resources must be nominal.

<AGENCY> management will resolve minimal and incidental use questions and issues in collaboration with <AGENCY>'s ISO, Human Resources Manager and Chief Counsel.

<AGENCY>
POLICY

INFORMATION SECURITY		**NUMBER:**	**xxxx**
		EFFECTIVE:	**mm/dd/yyyy**
		REVISED DATE:	**mm/dd/yyyy**
SUBJECT: ACCEPTABLE USE		**APPROVED:**	

SECTION 4 – ENFORCEMENT, AUDITING, REPORTING

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of <AGENCY> information resources access privileges, civil, and criminal prosecution.

   (Note: Agencies need to be aware of the constantly changing legal framework of the environment in which they operate, and they must adapt accordingly. Appropriate legal advisors and/or human resources representatives should review the policy and all of the procedures in use for policy enforcement. Some legal/human resources believe it is not necessary to include this section because all policy is enforceable. In fact, if it is included in one, it may be detrimental to the enforcement of other policies that do not include the section.)

2. <AGENCY> Management is responsible for the periodic auditing and reporting of compliance with this policy. <AGENCY> executives will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to <AGENCY> Management.
3. Exceptions to this policy will be considered only when the requested exception is documented using the Exception Handling Process and Form and submitted to the <AGENCY>'s ISO and <AGENCY>'s Policy Review Committee.
4. Intranet or by telephone at 555-5555.

SECTION 5 – REFERENCES

Government Code Section 8314

xxxx - Internet Use Standard

xxxx - Internet Content Filtering

xxxx – Electronic Mail Use Standard

xxxx - Intranet Use Standard

SECTION 6 – CONTROL AND MAINTENANCE

Policy Version: X.X.X
Date: mm/dd/yyyy
Author:
Owner: <AGENCY> ISO

<AGENCY> Policy will be reviewed and revised in accordance with parameters established in the Information Security Charter and Policy Management Process.

Glossary

Agency – When used lower case (agency), refers to any office, department, board, bureau, commission, or other organizational entity within state government. When capitalized (Agency), the term refers to one of the state's super agencies such as the State and Consumer Services Agency or the Health and Human Services Agency.

Availability – Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

Biometrics – A technology that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas, and hand measurements, while examples of behavioral characteristics include signature and typing patterns.

CCTV – An acronym for closed-circuit televisions used for surveillance.

Committee of Sponsoring Organizations (COSO) – The Treadway Commission's report on "The Internal Control – Integrated Framework" which defines internal control as a process and provides reasonable assurance regarding the achievement of objectives. See SAM Section 20050.

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

Continuity of Operations Plan (COOP)/ Continuity of Government (COG) – Ensures the continuity of essential functions through a wide range of emergencies and disasters.

Cryptography – A discipline of mathematics and computer science concerned with information security issues, particularly encryption and authentication use in access control.

Demilitarized Zone (DMZ) – A network area that sits between an organization's internal network and an external network, usually the Internet.

Firewall – A piece of hardware and/or software which functions in a networked environment to prevent communications forbidden by the security policy.

Federal Information Processing Standards (**FIPS**) – Publicly announced standards developed by the federal government for use by all non-military government agencies and by government contractors**.**

Guideline – A recommended course of action. Guidelines support the policy and the standards.

Health Insurance Portability and Accountability Act (**HIPAA**) – Requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

HVAC – An acronym for "Heating, Ventilation and Air-Conditioning," also referred to as climate control.

IDS/IPS – An Intrusion Detection System (IDS) is any device that generally detects unwanted manipulations to systems. An Intrusion Prevention System (IPS) is any device which exercises access control to protect computers from exploitation.

Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

Information Security Officer (ISO) – A position that focuses on information security within an organization. Required in state government as defined in SAM Section 5315.

ISO/IEC 27002 (formally 17799v2005) – An information security standard published in July 2007 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Malicious Code (Malware) – A program written to deliberately cause an unexpected and/or unwanted event on a computer or network, such as keystroke loggers, spy ware, viruses, worms, Trojan horses.

National Institute of Standardization and Technology (NIST) – The mission of the Federal NIST's Computer Security Division is to improve information systems security by raising awareness and conducting research for IT vulnerabilities; developing standards, metrics, tests and validation programs; and developing guidance to increase secure IT planning, implementation, management, and operation.

Payment Card Industry Data Security Standards (PCI DSS) – A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Policy – A broad statement authorizing a course of action to enforce an agency's guiding principles for a particular control domain. Policies are interpreted and supported by standards, guidelines, and procedures.

Procedure – provides instructions describing how to achieve a policy or standard. A procedure establishes and defines the process whereby a business unit complies with the policies or standards of the agency.

Process – A series of actions or operations conducing to an end; *especially* a continuous operation or treatment.

Supervisory Control and Data Acquisition Systems (SCADA) – A large-scale, distributed measurement and control system with processes based industrial, infrastructure or facility.

State Administrative Manual (SAM) – A State of California reference source for statewide policies, procedures, regulations, and information developed and issued by authoring agencies such as the Governor's Office, Department of General Services (DGS), Department of Finance (DOF), and Department of Personnel Administration (DPA).

Office of Information Security and Privacy Protection (OISPP) – Has statewide responsibility and authority over the information security policy identified in SAM Sections 5300 through 5399.

Statewide Information Management Manual (SIMM) – Contains instructions, forms, and templates that state agencies must use to comply with policy.

Smart Card – A pocket-sized card with embedded integrated circuits used for authentication purposes.

Systems Development Life Cycle (SDLC) – A process used to develop an information system, including requirements, validation, training, and user ownership through investigation, analysis, design, implementation, and maintenance.

Spyware – A broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user.

Standard – Applies to any definite rule, principle, or measure established by authority.

TCP/IP – An acronym for Transmission Control Protocol/Internet Protocol which is the Internet protocol suite of communications protocols that the Internet and most commercial networks run.

Token – A physical device that an authorized user of computer services is given to aid in authentication.

UPS – An acronym for Uninterruptible Power Supply, and a device or system that maintains a continuous supply of electric power to certain essential equipment that must not be shut down unexpected

References

All-In-One CISSP Exam Guide, Third Edition, Shon Harris, McGraw Hill, published 2005

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 17799:2005 standards

Department of General Services – SAM – www.sam.dgs.ca.gov/TOC/default.htm

County of Sacramento, “Anchor County of Sacramento, “Anchor Your Information Security Program” Booklet by Jim Reiner

Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST)

Wikipedia – www.wikipedia.com/

Merriam-Webster Online – www.merriam-webster.com/