
Information Technology Security Program Guideline

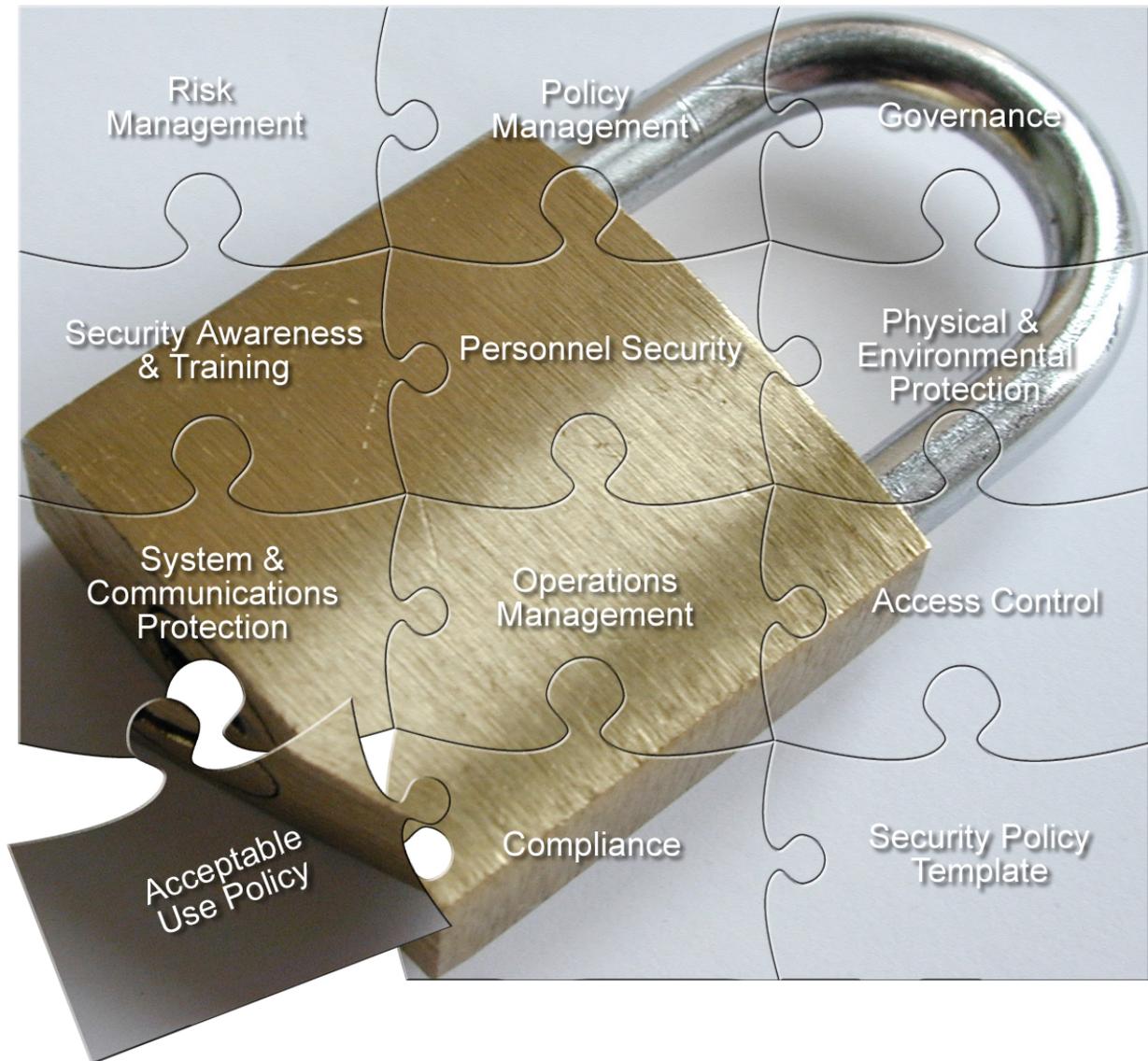


TABLE OF CONTENTS

- SCOPE & PURPOSE..... 1
- INTRODUCTION..... 2
- SECURITY COMPONENTS 3
 - Risk Management..... 3
 - Policy Management 4
 - Personnel Security..... 4
 - Physical and Environmental Protection 5
 - System and Communications Protection 6
 - Operations Management 7
 - Access Control 8
 - Security Awareness and Training 9
 - Governance 9
 - Compliance..... 10
- SECURITY POLICY TEMPLATE 11
- GLOSSARY 12
- APPENDIX A: Acceptable Use Security Policy 13
- APPENDIX B: Acknowledgements..... 18

SCOPE & PURPOSE

This Information Technology Security Guideline is applicable to all agencies that operate, manage, or use information technology to support business functions in the State of California.

This guideline lists the key components that need to be considered by an agency when implementing, reviewing or seeking to improve the value of its information security program. While not mandatory, it is highly encouraged that these components be reviewed for applicability to business environments, and implemented as appropriate for each agency. The authors (see Appendix B for workgroup members) recognize that all agencies may not require all components, but where a component is applicable to an agency's program, the best practices for that component should be assessed for implementation or adoption.

Further, this security guideline should not be misconstrued as superseding or alleviating agency responsibility for compliance with any existing legal or policy requirements.

This security guideline should be considered:

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

INTRODUCTION

This document will introduce the following ten core security components that should be considered when building a new security program or improving an existing one:

- Risk Management
- Policy Management
- Personnel Security
- Physical and Environmental Protection
- System and Communications Protection
- Operations Management
- Access Control
- Security Awareness and Training
- Governance
- Compliance

Together these components provide a framework that enable secure communications and appropriate protection of information resources within the State of California. In addition, they provide a basis for developing the agency's information technology security program and safeguard valuable information and system assets. For each component listed above, a best practices list has been identified that is strongly recommended, but which is not mandatory.

As industry standards and technology continue to evolve and mature, each agency needs to identify best practices to further strengthen their security program. However, given the diversity of business environments across the State, it is not practical to qualify all security best practices presented in this document or limit a security program to this set of best practices. A large percentage of State agencies will find significant value in formally adopting the best practices listed in this guideline as part of their security program.

Additionally, to aid with the development of consistent, well designed security policies, this document 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 ten core components into specific goals and objectives.

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. As it applies to IT systems, the National Institute of Standards and Technology (NIST) documented a risk management model that can be tailored to any size organization and encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

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. The risk assessment methodology encompasses 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 and assessment, is ongoing and evolving. Evaluation and assessment emphasizes the good practice to develop an effective risk management program within the department's IT security program. Not only should the risk management program engage changes to existing system, but should also integrate into the department's System Development Life Cycle (SDLC) for IT systems.

Best Practices

- Each agency should assign an individual, usually the ISO, responsible for risk assessment (SAM Section 4842.1).
- Through a comprehensive business impact analysis, each agency should identify their information assets, then categorize and prioritize these assets based on criticality (SAM Section 4842.1).
- In the context of the agency's planning, acquisition, and change management processes; cost-effective protective measures are to be selected and implemented (SAM Section 4842.1).
- Risk assessment results should be documented in a management report and submitted to the agency director (SAM Section 4842.1).
- The State has an IT Security Risk Assessment Checklist (SIMM Form 145) that an agency can use to build a risk assessment method specific to the agency's business programs and related information technology environment.

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 flexible and independent of specific hardware and software decisions to adapt to changes in your department's operating environment.

To be practical and effective, policies must be further defined by standards, guidelines, and procedures. These ensure that operations are consistent with the intent of the security policies.

Best Practices

- Create a process for adopting new policies and reviewing existing ones.
- Develop a formal approval process and identify individuals or roles that will approve new policies and change existing ones.
- Security Policy related processes should clearly identify what is to be performed, the frequency, and the position that is responsible to perform the process.
- Each agency should have policy and standards in place that clearly identify what can be performed, stored, accessed and used through the use of your department's computing resources (e.g., acceptable use policy, peer-to-peer policy, internet use policy).
- Policies should be reviewed periodically or when there have been changes in internal processes, laws or regulations, standards, or any changes to related policies.
- Once security policies and procedures have been established, they should be disseminated to all appropriate users, staff, management, and third party providers. Establish a record that those involved have read the policy.

Personnel Security

Personnel Security refers to those practices, technologies, and services to ensure the individuals authorized to access or maintain systems that use or process confidential and/or sensitive information have the appropriate clearances.

Personnel security assures that legitimate users have the appropriate system access necessary to perform their duties. Because of their internal access levels, authorized users pose a potential threat to systems and data. Employees, contractors, or third-party employees can exploit their legitimate computer access for malicious, fraudulent, or economic reasons. Additionally, reducing the amount of users with system administrator privileges reduces the risk of accidental damage or loss of information and systems.

Best Practices

- Position categorization for all positions should be completed to identify and assign risk.
- Appropriate background checks should be required for those that have access to confidential or sensitive data, or critical applications or systems.
- Remove 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 on use and access for non-state entities (including vendors and other contractors), that are documented in agreements to comply with all State policy and law regarding use of information resources and data. (SAM Section 4841.2).

Physical and Environmental Protection

Physical Security refers to those practices, technologies and services used to address the threats, vulnerabilities, and counter measures utilized to protect information assets.

Physical security safeguards take into account: 1) the physical facility housing the information resources; 2) the general operating location; and 3) any additional facilities that support the operation of the information systems (i.e. data centers).

Best practices can be separated into four categories: authorization, access controls, monitoring and logging.

- *Authorization* is the practice of ensuring that entry into an organization's facilities and restricted areas is done so with proper authorization.
- *Access control* is the practice of ensuring that entry into facilities is controlled and limited to personnel with proper authorization and credentials.
- *Monitoring* is the practice of ensuring that entry into an organization's facilities is monitored for breaches and/or compromises.
- *Logging* is the practice of ensuring that entry and access to facilities and Data Centers is logged for audit purposes.

Best Practices

- System components used to deliver *mission critical*, confidential, or sensitive programs should be located in a strategically placed, access controlled area. The placement might include an access restricted, windowless, temperature controlled area, with special floors, fire protection, HVAC, UPS and walls extending through the ceilings.
- Access to *non-mission critical* computer hardware, wiring, displays and network should be controlled by the principle of least privilege (e.g., assigned the fewest privileges consistent with their assigned duties and functions).
- System configurations (i.e., hardware, wiring, displays, and network) should be documented and treated as sensitive information. Any changes should be governed by a formal change management process.
- Physical access security for back-up systems, tapes and storage media should meet or exceed physical access security of the primary facilities and related access controls.
- Access to computer hardware, wiring, displays and networks should be monitored and audited (e.g., badges, cameras, access logs, sign-in sheets, etc.).
- Establish additional controls (e.g., CCTVs, cameras) and special access authorizations for restricted areas (e.g., network area, computer rooms, any area processing financial implements, such as cash or checks).
- Contracts for physical security services (e.g., Security Guards) should include language 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 portable computing devices (e.g., laptops, Blackberries, Treos) such as, but not limited to, locking cables, passwords and encryption.
- Develop, maintain, and regularly review a master list of access authorizations for each person and facility within an organization's infrastructure.

- Ensure badges and access codes are promptly deactivated 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.

System and Communications Protection

System and 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 data and systems is based on the classification and criticality of the data and the business processes that use the data.

The five key elements of system and communications protection are denial of service protection, boundary protection, use of validated cryptography, 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.

Best Practices

- Appropriate anti-virus, anti-spyware and file extension blocking solutions should be deployed and kept updated at the email gateway and on the desktop and server systems to prevent these systems from being compromised.
- Appropriate IDS/IPS solution should be deployed at the correct network location(s) and monitored to detect when the agency is under attack so an effective detection and defense strategy can be deployed.
- An agency should have a contingency plan for continuing service if they become a victim of a denial of service attack.
- A firewall or other boundary protection mechanism should be in place and must have the ability to evaluate (1) source and destination network addresses, and (2) determine the validity of the service requested.
- It may be necessary to firewall certain internal data and systems (Accounting and Personnel, for instance) from other data and systems on the networks.
- Cryptographic solutions should be in place when (1) the confidentiality information must be maintained while a message is in transit between computing devices and (2) when confidential information is stored in a file or database.
- Application servers, database servers, or infrastructure components containing any confidential or private data should not be exposed directly to the Internet. Components that meet these criteria are placed behind the Demilitarized Zone (DMZ) where they are not accessible from the internet and can only interact with DMZ components through a second and more restrictive firewall.
- Anti-spyware software should be deployed at either a gateway entry point of the network or at the desktop, and the software must be kept current.
- The agency ISO should use continual awareness messages as a defense mechanism to protect the agency from a successful malicious code attack.

Operations Management

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. But, as always, it is a balance of these types of controls against business requirements, cost, efficiency, and effectiveness.

Operations Management covers Information Technology 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 corporate 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 organization'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 organization's specific 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 data's 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 data be violated. The second item is the ongoing business need for the data, which is particularly relevant when continuous availability (i.e., round-the-clock processing) is required.

Best Practices

- Implement an appropriate level of security monitoring including intrusion detection, penetration testing, and violation analysis using either agency staff or third party managed services.
- Perform reviews of audit trails on a regular basis to alert an organization to inappropriate practices.
- Agencies should have preventive controls to decrease the threat of unintentional errors or unauthorized users accessing the system and modifying data.
- Agencies should have detection controls that help identify when an error has occurred.
- Use a system that provides a separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
- Data backup and restore procedures should be in place to reduce the likelihood of data loss.
- Agencies should have appropriate retention policies as dictated by organization policies, standards, legal and business rules.
- Agencies should have appropriate documentation such as organizational security policy and procedures, security, contingency, and disaster recovery plans.

Access Control

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

Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about what can be accessed. 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 component. 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 information technology.

Authorization is the process used to grant permissions to authenticated users. Authorization grants the person(s), technology, or process the right to use the information asset(s). Examples of the authorization process include signed access control forms for new employees and signed contracts between organizations granting information rights. 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 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 a login banner to display a general security notice and acceptance of conditions of use.
- Remove access upon employee termination or after 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.
- Automatic logout or protected screen savers should be initiated by the system after a specific period of inactivity.

Security Awareness and Training

Security Awareness and Training refers to the program used to promote awareness and responsibilities with regards to security risks related to the use and management of an agency's information resources. An effective security awareness and training program ensures people know about information security relative to their job responsibilities. The awareness program essentially markets the existing policies, standards, and practices. Information security can be a dry subject to some people; a program that knows its target audience and plans its message accordingly will reach more people.

A successful security awareness program should target various groups with information pertinent to their respective roles. Most people are end users that 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 information security, risk management, and business continuity.

Best Practices

- Promote security awareness using techniques such as: posters, email messages, formal instruction, web-based instruction, videos, newsletters, and security awareness days.
- Sign confidential and acceptable use statements annually.
- Train users to quickly identify threats, and how to respond to security incidents.
- Inform the users about agency policies and procedures.
- Regularly review and update training content to reflect changes to the agency's environment.

Governance

IT Security Governance enables the enterprise to take full advantage of its information, thereby maximizing benefits and capitalizing on opportunities. Furthermore, IT Security Governance integrates and institutionalizes good practices, and should also be aligned with the IT governance framework in an organization.

Governance maintains balance between the value of IT Security, the management of IT Security-related risks, and increased requirements for control over information. Value, risk and control constitute the core of IT Security Governance.

IT Security Governance is the responsibility of Senior Management and Executive Staff, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT Security Program sustains and extends the organization's strategies and objectives. Information security is a top-down process requiring a comprehensive security strategy that is explicitly linked to the organization's business processes and strategy. Security should address entire organizational processes, both physical and technical, from end to end. The tone at the top should be conducive to effective security governance. 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:

- 1) Achieving consensus in the organization by balancing the needs of your business against information security resources.
- 2) Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels;

- 3) Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care;
- 4) The structure and framework to optimize allocation of limited security resources;
- 5) Assurance of effective information security policy and policy compliance;
- 6) Reducing operational costs by providing predictable outcomes—mitigating risk factors that may interrupt the business process; and
- 7) Improving trust in customer relationships, and protecting the organization's reputation.

Best Practices

- Designate an individual to fulfill the role of Senior/Chief Information Security Officer, who should be directly responsible to the agency director for this purpose (SAM Section 4841.1), and who should possess professional qualifications, including the training and experience required to administer an information security program as defined in this document.
- Require regular reports from the Senior/Chief Information Security Officer on the program's adequacy and effectiveness.
- Regularly review investment in information security to ensure continued alignment with the agency business program strategies and objectives.

Compliance

Compliance refers to the process framework for ensuring conformity to applicable state security policies and verifying adherence to statewide reporting requirements. The following is not a list of best practices, rather required policy, set forth by the Department of Finance in the State Administration Manual (SAM) Section 4845, 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 IT security program compliance and shall take reasonable measures to implement and report according to the following:

Requirements

- As noted in SAM Section 4843.1, each agency must file an informational copy of its Operational Recovery Plan with the Department of Finance by the due date outlined in the Operational Recovery Plan Quarterly Reporting Schedule (SIMM Section 05).
- 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 within two hours of discovery.
- By January 31 of each year, or as instructed by the Department of Finance, the director of each agency must certify that the agency is in compliance with state policy governing information technology risk management by submitting the Risk Management Certification (SIMM Section 70).
- By January 31 of each year or as instructed by the Department of Finance, the director of each agency must certify and provide the name, title, business address, IMS code, email address, and telephone number of the agency's Information Security Officer and/or the Operational Recovery Coordinator on the form specified in SIMM Section 70.
- Known instances in which you suspect personal information has been distributed by the agency or obtained by any person in a manner not in accordance with law (Information Practices Act and the California Public Records Act) require reporting to the California Highway Patrol.

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.

The security policies developed must establish a consistent notion of what is and what is not permitted with respect to control of access to your information resources. They must bond with the business, technical, legal, and regulatory environment of your agency.

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

Section 1 – Introduction:

A purpose should be stated in the introduction section. This should provide the reader with a brief description of what this policy will state and why it is needed. The security stance of your agency should be stated here.

Section 2 – Roles and Responsibilities:

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

Section 3 – Policy Directives:

This section describes the specifics of the security policy. It should provide sufficient information to guide the development and implementation of guidelines and specific security procedures.

Section 4 – Enforcement, Auditing, Reporting:

This section states what is considered a violation and the penalties for non-compliance. The violation of a policy usually implies an adverse action which needs to be enforced.

Section 5 – References:

This section lists all references mentioned in the policy, including agency standards, procedures, government code, and State Administrative Manual sections.

Section 6 – Control and Maintenance:

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

GLOSSARY

Biometrics – is 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 – is an acronym for closed-circuit televisions used for surveillance.

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

Demilitarized Zone - is a network area that sits between an organization's internal network and an external network, usually the Internet.

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

Guideline - is a recommended course of action. Guidelines support the policy and the standards.

HVAC - is an acronym that stands for "heating, ventilation and air-conditioning". This is sometimes 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.

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

Procedure - A 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.

SAM - The State Administrative Manual (SAM) is 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.

SIMM - The Statewide Information Management Manual (SIMM) contains instructions, forms and templates that State agencies must use to comply with Information Technology (IT) policy.

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

Spyware – is 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.

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

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

UPS – is an acronym for uninterruptible power supply, and is a device or system that maintains a continuous supply of electric power to certain essential equipment that must not be shut down unexpectedly.

APPENDIX A: Acceptable Use Security Policy

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 with the development of your own agency Acceptable Use Security Policy by giving specific examples of what can be performed, stored, accessed and used through the use of your departments computing resources.

**<AGENCY>
POLICY**

INFORMATION SECURITY

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

SUBJECT: ACCEPTABLE USE

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 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 individuals who may use information resources with respect to their responsibilities associated with computer resource use.

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

Section 2 – Roles & 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 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

1. <AGENCY> will establish formal Standards and Processes to support the ongoing development and maintenance of the <AGENCY> Acceptable Use Policy.
2. The <AGENCY> Director and Management will commit to the ongoing training and education of <AGENCY>e 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
3. The <AGENCY> Director and Management will use metrics to establish the need for additional education or awareness program in order to facilitate the reduction in the threat and vulnerability profiles of <AGENCY> Assets and Information Resources.
4. The <AGENCY> Director and Managers will establish a formal review cycle for all Acceptable Use initiatives.

**<AGENCY>
POLICY**

INFORMATION SECURITY

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

SUBJECT: ACCEPTABLE USE

5. Any security issues discovered will be reported to the CISO or his 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 such 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 CISO..

**<AGENCY>
POLICY**

INFORMATION SECURITY

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

SUBJECT: ACCEPTABLE USE

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 CISO or his designee for follow-up investigation. Additional Reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.

Part IV – Incidental Use

Government Code Section 8314 permits incidental personal use of state resources. At <AGENCY> this means:

1. Incidental personal use of electronic mail, 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. Incidental use must not result in direct costs to <AGENCY>, cause legal action against, or cause embarrassment to <AGENCY>
3. 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 incidental use questions and issues using these guidelines in collaboration with <AGENCY>'s CISO, HR Manager and Chief Counsel.

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.

**<AGENCY>
POLICY**

INFORMATION SECURITY

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

SUBJECT: ACCEPTABLE USE

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> Chief Information Security Officer and <AGENCY> Policy Review Committee.
4. Any employee may, at any time, anonymously report policy violations via <AGENCY>'s Intranet or by telephone at 555-5555.

Section 5 - References

Government Code Section 8314

xxxx - Internet Use Standard

xxxx - Internet Content Filtering

xxxx - E-Mail Use Standard

xxxx - Intranet use Standard

Section 6 - Control and Maintenance

Policy Version: X.X.X

Date: mm/dd/yyyy

Author:

Owner: <AGENCY> CISO

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

APPENDIX B: Acknowledgements

This document would not have been possible without the tireless efforts of the following workgroup members:

Darin Arcolino, Employment Training Panel

Thys Bohr, California Department of Veterans Affairs

Stephanie Cervantes, State Controller's Office

Ryan Dulin, Department of Finance

Bill Howe, Department of Technology Services

Paulette Johnson, Department of Motor Vehicles

Tony Lourick, Department of Water Resources

Patrick McGuire, Franchise Tax Board

Tony Poon, Department of Finance

Rosa Umbach, Office of Statewide Health Planning and Development