

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

**CHAPTER 5100 INDEX**

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

**IT STANDARDS**

<b>POLICY</b>	<b>5100</b>
<b>COMPUTER PROGRAMMING LANGUAGES</b>	<b>5101</b>
<b>Open Data Policy Introduction</b>	<b>5160</b>
<b>Open Data Policy Requirements</b>	<b>5160.1</b>
<b>Open Data Exceptions</b>	<b>5160.2</b>
<b>Workgroup Collaboration Platform Policy</b>	<b>5170</b>
<b>Operating Software, Utilities And Programming Aids</b>	<b>5175.1</b>
<b>Application Packages</b>	<b>5175.2</b>
<b>COMPLIANCE WITH UNITED STATES POSTAL SERVICES, OPTICAL CHARACTER RECOGNITION GUIDELINES</b>	<b>5179</b>
<b>UNITED STATES POSTAL SERVICE ZIP + 4 GUIDELINES</b>	<b>5180</b>
<b>WEBSITE STANDARDS INTRODUCTION</b>	<b>5190</b>
<b>Website Standards</b>	<b>5190.1</b>
<b>California State Website Template</b>	<b>5190.2</b>
<b>INTERNET DOMAIN NAME</b>	<b>5195</b>
<b>Internet Domain Name Requirements</b>	<b>5195.1</b>
<b>Internet Domain Name Annual Certification</b>	<b>5195.2</b>

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

**POLICY**

**5100**

(Revised 3/2011)

The Department of Technology embraces the American National Standards Institute ([ANSI](#)) management information standards and the Federal Information Processing Standards ([FIPS](#)). The ANSI standards are national consensus standards which provide guidance on a variety of issues central to the public and industrial sectors. The FIPS standards are adopted and promulgated under the provision of Public Law 89–306 (Brooks Act) and [Part 6 of Title 15, Code of Federal Regulations](#), and serve to improve the utilization and management of computers and automated data processing in the Federal Government.

State agencies must use the ANSI and FIPS standards in their information management planning and operations. Adoption of these standards will facilitate the inter organizational sharing and exchange of equipment, data, software and personnel.

Use of these standards will also facilitate communication (1) among state agencies; (2) between the state and its IT vendors; and (3) between the state and its IT information providers/recipients.

**COMPUTER PROGRAMMING LANGUAGES**

**5101**

(Revised 3/2011)

The Department of Technology encourages the use of vendor supplied packages versus in-house development whenever vendor supplied packages can be demonstrated to be the most cost beneficial solution to IT project problems or opportunities.

**OPEN DATA POLICY INTRODUCTION**

**5160**

(Revised 03/2019)

The Public Records Act, Government Code (GC) Sections 6250- 6270, provides public access to information that is collected and maintained by state and local entities, mindful of the right of individuals to privacy. The State of California is committed to unlocking the value of government data to propel innovation, improve the delivery of public services and empower the people of California while protecting privacy. Information is a valuable resource and a strategic asset to State Government, its partners, and the public. Managing government information as an asset will increase operational efficiencies, enhance performance planning, improve services, support mission needs, inform policy decisions, safeguard personal information, and increase public access to valuable government information. Open data helps ensure that all public datasets are discoverable and fuels entrepreneurship, economic development and scientific discovery. To ensure that State Government is taking full advantage of its information resources, Agencies/state entities shall manage their data as an asset from the start and, wherever possible, release it to the public in a way that makes it open, discoverable and usable.

**OPEN DATA POLICY REQUIREMENTS**

**5160.1**

(Revised 03/2019)

Effective July 1<sup>st</sup>, 2019, as part of the Open Data policy, each Agency/state entity shall:

1. Build or modernize Information Technology (IT) solutions in a way that maximizes interoperability and information accessibility. Although this policy does not require Agency/state entities to modernize existing IT solutions, it does require data considerations identified in this section be applied when a state entity undertakes a modernization effort that substantially modifies an existing IT solution.
  - a. Exercise forethought when architecting, building, or substantially modifying an IT system to facilitate data distribution to the public, where appropriate.
  - b. Use machine-readable and open formats for information as it is collected or created. Where applicable, machine-readable and open formats must be used in conjunction with electronic or paper-based information collection efforts.
  - c. Prioritize the use of open formats that are non-proprietary, publicly available, and that place no restrictions upon their use.
  - d. Apply open licenses, such as Creative Commons Zero (CC0), to information as it is collected or created so that if data are made public there are no restrictions on copying, publishing, distributing, transmitting, and adapting.
  - e. Systems must be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design (e.g. leveraging standards and industry best practices for information sharing, separation of data from the application layer to maximize data reuse opportunities.)
2. Whenever feasible, make data broadly available to the public through the Agency/state entity's open data site or portal, pursuant to the limited exceptions outlined in SAM Section 5160.2.
3. Describe information using standard metadata as the data is collected or created.
  - a. Open Data shall include Project Open Data Catalog Vocabulary (DCAT) standards modified for California, see [Open Data Handbook](#) for specifications and formats.
  - b. Agencies/state entities may expand upon metadata and data dictionaries based on standards, specifications, or formats developed within different communities (e.g., financial, health, geospatial, law enforcement). Groups that develop and promulgate these metadata specifications must review them for compliance with DCAT specifications and formats

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

(Continued)

**OPEN DATA POLICY REQUIREMENTS**  
(Revised 03/2019)

**5160.1 (Cont. 1)**

- c. Metadata and data dictionaries shall be in a machine-readable format to provide users the ability to export when needed.
4. Adopt effective governance and data asset portfolio management approaches, including data management and release practices to ensure consistency.
  - a. Create and maintain an Agency/state entity enterprise data inventory, see [Open Data Handbook](#) for inventory specifications and formats.
  - b. The inventory shall indicate, as appropriate, if the Agency/state entity has determined that the individual datasets may be made publicly available (i.e., release is permitted by law, subject to all privacy, confidentiality, security, Agency/state entity has ownership of data, and other valid requirements) and whether they are currently available to the public.
  - c. The inventory shall list any datasets that can be made publicly available at the Agency/state entity's open data site or portal in a format that enables automatic aggregation by Data.ca.gov and other services (known as "harvestable files"), to the extent practicable. See [Open Data Handbook](#) for best practices, tools, and schema to implement the public data listing and harvestable files.
  - d. Public data listing should include, to the extent permitted by law and existing terms and conditions, datasets that were produced as a result of legislative mandates, state grants, contracts, and cooperative agreements (excluding any data submitted primarily for the purpose of contract monitoring and administration), and, where feasible, be accompanied by standard citation information, preferably in the form of a persistent identifier.
  - e. Assign a Data Coordinator to coordinate and maintain Agency/state entity's public data. The Data Coordinator's contact information must be identified in the enterprise data inventory.
5. Prioritize the collection of data sets.
  - a. Agencies/state entities shall identify and engage stakeholders as part of the intake process.
  - b. Create a process to engage with customers to solicit help in identifying data sets of value to the public, in prioritizing the release of public datasets

(Continued)

**OPEN DATA POLICY REQUIREMENTS**

**5160.1 (Cont. 2)**

(Revised 03/2019)

and determining the most usable and appropriate formats for release. Agencies/state entities should make public data available in multiple file formats according to their customer needs (e.g. high-volume datasets of interest to developers should be released using bulk downloads as well as Application Programming Interfaces (APIs)).

6. Ensure that privacy and confidentiality are fully protected, and that data is properly secured.
  - a. Leverage an internal data governance process to determine if information collected or created can be made publicly available or is subject to restrictions (e.g. privacy, confidentiality, security, trade secret, contractual). See [Open Data Handbook](#) for additional information.
  - b. If the Agency/state entity determines that information should not be made publicly available on one of these grounds, the Agency/state entity must document this determination through its internal data governance process.
  - c. Consider security-related restrictions including National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199 “Standards for Security Categorization of Federal Information and Information Systems,” which includes guidance and definitions for confidentiality, integrity, and availability.
  - d. Collect or create only that information necessary for the proper performance and evaluation of Agency/state entity functions and which has practical utility. Limit the collection or creation of information which identifies individuals to that which is legally authorized and necessary for the proper performance of Agency/state entity functions.
  - e. Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists. [Data sharing agreements](#) must be created to exchange information across Agencies/state entities and with research institutions in compliance with the State’s information security and privacy policy and standards, see SAM Section 5300 and Statewide Information Management Manual (SIMM) Section 5305-A.
  - f. Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. Agencies/state entities shall consider the standard for information classification detailed in SIMM Section 5305-A and other publicly available information when determining whether information should be considered Personally Identifiable Information.

**OPEN DATA EXCEPTIONS**

**5160.2**

(Revised 03/2019)

The Information Practices Act (IPA) of 1977 (Civil Code Section 1798, et seq.) provides measures to assure fair treatment of individuals who are the subject of state entity records, providing specific requirements for the collection, use, maintenance and dissemination of information relating to individuals. Nothing in SAM Section 5160 shall be construed to require Agencies/state entities to make data available to the public, if, on the facts of the particular case, disclosure of that data would increase the potential to harm an Agency/state entity or the public. The exceptions provided below may be applied, in specific instances, to exempt an Agency/state entity from sharing data with the public. Any exceptions used must be approved through the Agency/state entity's internal data governance process and documented in the enterprise data inventory for the purposes of ensuring effective oversight and management of information assets.

Applicable exceptions are as follows:

1. The sharing of the data is restricted by statute, practice or legal precedent, including—but not limited to—patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulation, and the Federal laws and regulations governing classified information;
2. The sharing of the data would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy;
3. The sharing of the data would create an identifiable risk to the stability, security, or integrity of the Agency/state entity's systems or personnel;
4. The sharing of data would create an identifiable risk to the Agency/state entity's mission, programs, or operations.

**WORKGROUP COLLABORATION PLATFORM POLICY**

**5170**

(New 01/2020)

The increased utilization of collaborative tools that emphasize and enable teamwork continues to improve the way government communicates and collaborates. Unified communications platforms promote capabilities that allow remote collaboration. These platforms combine features such as chat, conferencing, calendaring, notes, and attachments into a single enterprise platform enabling the rapid provisioning of shared workspaces and facilitating distribution of topic based information.

Each agency/state entity shall develop and implement internal policies and procedures to ensure proper use of Workgroup Collaboration Platforms, as defined in SAM Section 4819.2. These policies and procedures must comply with SAM Sections 4846 and 5300, which provide that all computer software purchased with state funds is procured in accordance with state law and used in compliance with licenses, contract terms and applicable copyright laws. In addition, management should ensure all staff understand and adhere to proper software management policies which address, at a minimum, the following key areas: acceptable use, public records act considerations, key roles and responsibilities, security/privacy, workspaces and records retention and management of Workgroup Collaboration Platforms. Statewide Information Management Manual (SIMM) Section 130 provides guidelines to assist agencies/state entities in developing policies and procedures for the proper use of Workgroup Collaboration Platforms.

**OPERATING SOFTWARE, UTILITIES AND PROGRAMMING AIDS** 5175.1  
(Reviewed 3/2011)

It is state policy that standard, unmodified, vendor-supplied-and-maintained software aids be used in lieu of developing unique programs. The objective is to minimize and control the development of specialized programs that allocate, schedule and control the CPU, memory, peripherals, communication, data storage and retrieval.

**APPLICATION PACKAGES** 5175.2  
(Reviewed 3/2011)

It is the state policy that all feasibility studies will address the availability, usability, maintainability and cost effectiveness of prewritten and tested application programs in lieu of developing major programs in-house. The objective is to minimize the development time and costs of major application programs when such programs are available from other sources.

**COMPLIANCE WITH UNITED STATES POSTAL SERVICE,  
OPTICAL CHARACTER RECOGNITION GUIDELINES** 5179  
(Reviewed 3/2011)

The United States Postal Service ([USPS](#)) has adopted guidelines to allow for optical character recognition of alphanumeric data contained in mailing addresses. Government agencies are strongly encouraged to follow these guidelines as a means of ensuring more efficient and accurate mail processing; more consistent mail delivery; and more stable postal operating costs.

To the extent that it is determined to be cost-effective, agencies must follow the USPS Optical Character Recognition (OCR) guidelines in the design and operation of automated information systems that include preparation of mailing addresses.

The OCR guidelines apply to letter mail within the following dimensions;

1. Height at least 3–1/2" and no more than 6–1/8";
2. Length at least 5" and no more than 11–1/2";
3. Thickness at least 0.007" and no more than 0.25"; and,
4. Aspect ratio (length divided by height) of from 1.3 to 2.5.

The details of the guidelines are set forth in the USPS publication, "A Guide to Business Mail Preparation" ([Publication 25](#)), which is available without charge. Agencies should contact their USPS Commercial Account Representative to obtain the current edition.

**UNITED STATES POSTAL SERVICE ZIP+4 GUIDELINES**  
(Reviewed 3/2011)

**5180**

The USPS offers a reduced postage rate to organizations for first-class mailings that use the 9-digit zip code (ZIP +4) in the mailing address. Both unsorted and sorted mailings are eligible for the reduced rate.

To the extent that it is cost-effective (taking into account the potential postage discount), agencies must provide for ZIP + 4 address coding and sorting of printed addresses in ZIP + 4 order in the design and operation of automated information systems that include preparation of mailing addresses.

There are two preliminary requirements for eligibility for the ZIP + 4 discount;

1. "Machinability," which includes quality of paper stock and adherence to the USPS standards for envelope size; and,
2. Optical Character Recognition (OCR) readability, which consists of adherence to the USPS OCR mailing guidelines.

Detailed specifications for these and other ZIP + 4 requirements are available from the USPS Commercial Account Representative assigned to each agency. Additional information is also contained in Section 324 of the [USPS Domestic Mail Manual](#).

**WEBSITE STANDARDS INTRODUCTION**

**5190**

(Revised 3/2019)

Websites are an essential tool for government to interact with the public and deliver information and services to the people of California. The Website Standards policy is designed to strengthen the security, usability, accessibility and quality of State of California websites through standardization and adoption of best practices. This policy will foster a consistent look and feel and a common navigational framework across government, helping users recognize they are accessing official State of California information. This policy also encourages Agencies/state entities to design and develop websites that are accessible to people with disabilities and promotes the adoption of usability principles that adhere to California's usability standards for website development.

**WEBSITE STANDARDS**

**5190.1**

(Revised 8/2018)

As part of the Website Standards Policy, Agencies/state entities must incorporate the mandatory website elements identified in this section for all public-facing websites within the CA.GOV domain. These elements include the following requirements: design, accessibility, domain, profile, usability, security, and analytics. See [webstandards.ca.gov](http://webstandards.ca.gov) for standard and web template resources.

**Mandatory Website Elements:**

1. **Design:** Websites shall include a strong brand presence for the State of California and

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

the Agency/state entity. The use of consistent design elements will help promote a standard look-and-feel while also improving the overall user experience.

- a. **Header** – The header provides a consistent, seamless look-and-feel to the State’s web presence. Key elements of the header shall include:
  - i. State Branding – The CA.GOV logo shall be placed in the top left corner of the header area inside a horizontal band that is at least 40 pixels high. The CA.GOV logo must be at least 34 pixels high and contain a hyperlink to the CA.GOV web portal. A hypertext only link is not permitted in place of the hyperlinked graphic logo image.
  - ii. Agency/state entity Branding – An Agency/state entity logo must be used for identification. The logo must be clear and contain legible text. When an Agency/state entity logo is not available, the state seal should be used in its place followed by the Agency/state entity title.
  - iii. Navigation – Provide a direct link to the most utilized landing pages or services within the website. Ensure link names are clear and concise and accurately represent the destination content. Ensure that the primary and secondary navigational elements are consistent and provides navigation on all webpages throughout the website.
  - iv. Search – A search button or hyperlink must be present inside the main navigation or header area.
  
- b. **Footer** – The footer must appear at the bottom of all Agency/state entity web pages. Key elements of the footer shall include:
  - i. Link to Agency/state entity’s Privacy Policy specific to the published website.
  - ii. Link to Agency/state entity’s Conditions of Use specific to the published website.

Contact information or link to contact information. Contact information must identify the name of the Agency/state entity that owns the website so there is no question as to which Agency/state entity the user may contact.
  - iii. Online Voter Registration hyperlink to the California Secretary of State’s [Online Voter Registration webpage](#).
  - iv. Link to user visible sitemap which presents a systematic hierarchical view of the website. The sitemaps shall be made available to users and search engine crawlers. A user visible sitemap, which presents a systematic hierarchical view of the website, shall be linked in the footer section. A user visible sitemap does not need to contain every page on the website if there are a large number of resources, especially application generated dynamic pages. A system or XML sitemap shall be available and placed into the root folder of the website and should include all of the available links. Sitemaps shall regularly be updated when new pages are published. It is recommended that XML sitemaps be submitted to all major search engines.
  - v. Link to Website Accessibility Certification, see [SAM Section 4833.2](#).



SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

available to desktop devices.

- b. **User Feedback** – Leverage user feedback and analytics to prioritize the modernization and optimization of legacy websites and digital services that are most frequently accessed by users.
  - c. **Usability Principles** - Leverage State web usability principles and standards featured at [WebStandards.ca.gov](http://WebStandards.ca.gov) and Federal principles featured at [usability.gov](http://usability.gov).
5. **Security:** Agencies/state entities must protect user privacy, data integrity and sensitive information. Key elements of website security shall include:
6. **Transport Layer Security** - Websites shall, at minimum, use Transport Layer Security (TLS) certificates (formerly referred to as Secure Socket Layer (SSL) certificates) that adhere to a minimum Secure Hash Algorithm (SHA) 2 and 2048-bit key encryption. At minimum the full Agency/state entity name shall be provided as the “unit” for TLS certificate purposes. The contact person(s) named in a TLS certificate must be consistent with the contact(s) registered for the domain. Agency/state entities shall verify contacts are consistent as part of the annual Domain Name Certification process, see SAM Section 5195.
- a. **Extended Validation** - Websites that process, store or transmit financial transactions and/or Personal Information, as defined by Civil Code Section 1798.3, shall use an Extended Validation (EV) TLS certificate.
7. **Analytics:** Agencies/state entities must participate in statewide analytics by deploying the statewide analytics tracking code on all public-facing websites. Participation in statewide analytics does not preclude Agency/state entities from using other analytics programs. The statewide analytics tracking code is available at [WebStandards.ca.gov](http://WebStandards.ca.gov).

**Optional Website Elements:**

Agencies/state entities are encouraged, but not required, to include the following elements in the content area of their websites:

1. Governor’s picture/graphical banner near the top of the content area.
2. Agency Secretary and/or State Entity Director’s picture/banner (or equivalent).
3. Essential Services highlighting key information of importance to the Agency/state entity.
4. Tribal Liaison contact information on the contact page.
5. Small Business & Disabled Veteran Business Enterprise (DVBE) Advocate Information on the contact page if applicable.

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

(New 7/2018)

Agencies/state entities are strongly encouraged to use the latest version of the standard CA.GOV website template to achieve many of the requirements identified in SAM Section 5190.1. The standard template is designed to promote a responsive and standard look and feel to ensure a uniform user experience. The template includes many usability, security and accessibility requirements and is updated regularly to meet evolving industry standards and best practices. Agencies/state entities that utilize the standard CA.GOV website template shall ensure that the latest version of the template is implemented within one year from the date of the latest template release.

The standard CA.GOV website template and instructions related to this policy can be found at [WebStandards.ca.gov](http://WebStandards.ca.gov). This online resource is a toolkit that provides standards, code, functionality, implementation guidelines and best practices for Agencies/state entities to implement the Website Standards policy.

**INTERNET DOMAIN NAME REQUIREMENTS**

**5195.1**

(New 5/2017)

California Department of Technology approval is required for any state entity, city, county, and government group that requests to use the ca.gov web domain. Web domains occupying the ca.gov domain zone must comply with all of the following requirements. See SIMM [Section 40A](#) for additional information on naming conventions and protocols.

- Domain names must be owned by a California state entity, county, city, or government group.
- Domain names must be organizationally or functionally identifiable and derived from the official name of the organization.
- Domain names must be consistent with federal policy and guidelines including, but not limited to, [41 Code of Federal Regulations, Part 102-173](#) and the Federal Interagency Committee on Government Information's Recommendations for Federal Public Websites.
- All websites in the "ca.gov" DNS Zone must contain a direct link to [www.ca.gov](http://www.ca.gov) and must provide both general information and details on digital services to be used on [www.ca.gov](http://www.ca.gov).

**INTERNET DOMAIN NAME ANNUAL CERTIFICATION**

**5195.2**

(New 5/2017)

All entities that use the ca.gov web domain are required to annually certify compliance with federal policy and guidelines and confirm that domain contact information is current. Any entity that fails to complete this annual certification requirement risks having their ca.gov domain name removed. See SIMM [Section 40A](#) for additional information and instructions regarding the annual certification process.

SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)

**INTERNET DOMAIN NAME POLICY**  
(New 5/2017)

**5195**

The State of California has been authorized to administer the “ca.gov” Domain Name Service (DNS) Zone by the United States General Services Administration (GSA). Web domains occupying this zone can only be acquired by an official state entity, county, city or government group within the State of California. The Government Operations Agency (GovOps) has statewide responsibility to oversee the ca.gov domain name program and the California Department of Technology will manage the registration, change, and renewal process for ca.gov domains. This policy applies to all second-level and third-level domain names within the ca.gov domain.