

**SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)**

**POLICY**  
(Reviewed 1/2016)

**4983.1**

As part of the Cloud First policy, each Agency/state entity shall:

1. Evaluate, in consultation with their IT organization, secure cloud computing alternatives for all reportable and non-reportable IT projects.
2. Use a cloud service model, i.e., Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), or Cloud Infrastructure as a Service (IaaS), for all new reportable and non-reportable IT projects whenever a feasible and cost effective solution is available that meets the Agency/state entity requirements, and provides the required level of security, performance and availability, and is consistent with the factors described in SAM [4981.1](#).
3. Use cloud services provided through the Office of Technology Services (OTech) as the first choice when implementing cloud computing solution for all new IT projects. If required services are not available through OTech, use other commercially available SaaS, PaaS or IaaS solutions.
4. Use commercially available SaaS services provided through OTech as the first choice for commodity applications such as common productivity software, email\* (including tools that integrate with email), virtual desktop, customer relationship management, human resources management, financial, project management, open data, and inventory management (refer to National Institute of Standards and Technology (NIST) Special Publication [800-146](#) for candidate SaaS application classes). If required services are not available through OTech, use other commercially available SaaS solutions. Use a PaaS or an IaaS service model for all other application categories when feasible.

\*Per Chapter 404, Statutes of 2010 (Assembly Bill 2408), all Agencies/state entities within the executive branch that are under the direct authority of the Governor must consolidate to the state's shared e-mail solution.

5. Classify the data managed by the applications that utilize cloud service models in accordance with SAM [5305.5](#).
6. Ensure compliance with the security provisions of the SAM (Chapters [5100](#) and [5300](#)) and the [SIMM](#) (Sections 58C, 58D, 66B, 5305A, 5310A and B, 5325A and B, 5330A, B and C, 5340A, B and C, 5360B).
7. Based on data classification pursuant to SAM 5305.5, ensure compliance with relevant security provisions including those in the California Information Practices Act (Civil Code Section [1798](#) et seq.), Internal Revenue Service (IRS) Publication [1075](#), Social Security Administration ([SSA](#)) Electronic Information Exchange Security Requirements, Payment Card Industry Data Security Standard (PCI DSS) including the PCI DSS Cloud Computing Guidelines, Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Health Information Technology for Economic and Clinical Health (HITECH) Act, and Criminal Justice Information Services (CJIS) Security Policy.

(Continued)

**SAM – INFORMATION TECHNOLOGY  
(California Department of Technology)**

(Continued)

**POLICY**

(Revised 1/2016)

**4983.1 (Cont. 1)**

8. Ensure appropriate level of compliance with the Federal Risk and Authorization Management Program (FedRAMP) certification for all IT projects using commercial cloud solutions where federal funding is involved.
9. Ensure that the commercial cloud service provider's Standards for Attestation Engagements No. 16 Service Organization Control (SOC) 2 Type II report along with the cloud service provider's plan to correct any negative findings is available to the Agency/state entity.
10. Ensure that the confidential, sensitive or personal information is encrypted in accordance with [SAM 5350.1](#) and [SIMM 5305-A](#), and at the necessary level of encryption for the data classification pursuant to [SAM 5305.5](#).
11. Ensure that written agreements with cloud service providers address SAM 5305.8 provisions, and SaaS service agreements include the Department of General Services' Cloud Computing Services Special Provisions.
12. Ensure that the physical location of the data center where the data is stored is within the continental United States, and remote access to data from outside the continental United States is prohibited unless approved in advance by the State Chief Information Security Officer.
13. Maintain an exit strategy for IT projects that utilize a commercially available SaaS service model. The exit strategy includes the Agency's/state entity's ability to export data in pre-defined formats and maintaining, when needed, a current backup of the data in the Tier III-equivalent data center facility designated to the Agency/state entity by [SAM 4982.1](#) and unrelated to the cloud provider.
14. Maintain an effective incident response and mitigation capability for security and privacy incidents in accordance with [SAM 5340](#). Report suspected and actual security incidents in accordance with the criteria and procedures set forth in SIMM 5340-A and other applicable laws and regulations.