POLICY **4983.1**
(Revised 08/2017)

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

1. Evaluate, in consultation with their IT organization, secure cloud computing alternatives for all IT projects and infrastructure initiatives (e.g., storage, servers, and Wide Area Network equipment).
2. Use a cloud service model, i.e., Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS), whenever a feasible and cost effective solution is available. The use of cloud services must be consistent with the factors described in SAM 4981.1.
3. Use IaaS or PaaS solutions for new, expansion or refresh initiatives.
4. Use IaaS and PaaS solutions provided through the California Department of Technology (CDT). Requests shall be submitted to CDT through a Remedy Service Request.
5. If required IaaS or PaaS solutions are not available through CDT, CDT will partner with the Department of General Services (DGS) to determine the best procurement method.
6. Use SaaS solutions provided through CDT, e.g., all office productivity software (including email*), or through DGS' Software Licensing Program (SLP), when implementing commercial and/or government SaaS cloud computing solutions.

   *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 share e-mail solution.
7. If required SaaS solutions are not provided through CDT, Agencies/state entities may acquire other commercial and/or government SaaS solutions.
8. If an Agency/state entity determines that the use of a cloud service solution is not feasible, or the required solution is not provided through CDT, they shall submit an exemption request to CDT for approval. The Cloud Computing Exemption Process is defined in Statewide Information Management Manual (SIMM) 18.
9. Classify the data managed by the applications that utilize cloud service models in accordance with SAM 5305.5.
10. 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).

(Continued)

11. 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.
12. Ensure that the commercial and/or government 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.
13. Ensure that all 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.
14. Ensure cloud service agreements include all of the DGS' Cloud Computing Services Special Provisions, and all written agreements with cloud service providers address SAM 5305.8 provisions.
15. 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.
16. Maintain an exit strategy for IT solutions that utilizes a commercial and/or government cloud service. The exit strategy must include the Agency's/state entity's ability to export data in pre-defined formats and maintain, when needed, a current backup of the data in the Agency/state entity's designated Tier III-equivalent data center facility. Designated data center facilities must be unrelated to the cloud provider; data center assignments are described in SAM 4982.1
17. 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.