

SAM – INFORMATION SECURITY (Office of Information Security)

INFORMATION SECURITY INTEGRATION

5315

(Revised 10/18)

Policy: Each state entity is responsible for the integration of information security and privacy within the organization. This includes, but is not limited to, the designing of appropriate security controls in new systems, or systems that are undergoing substantial redesign, including both in-house and outsourced solutions. Each state entity shall ensure its ISO, and where applicable its Privacy Program Coordinator and Technology Recovery Coordinator, are actively engaged with the owners of information, and project, procurement and technical personnel involved with information asset acquisition, development, operations, maintenance and disposal to:

1. Ensure information security is considered throughout the asset lifecycle, from acquisition and development through maintenance and operations, to retirement.
2. Integrate information security design requirements into both manual information handling and information processing functions, and information technology activities, including throughout the system development lifecycle (SDLC);
3. Create system security plans outlining key information security controls to mitigate risks;
4. Create and maintain residual risk documentation consistent with the State Information Management Principles, Record of Decisions (SAM Section [4800](#));
5. Integrate information security (confidentiality, integrity, and availability) requirements into contracts for outsourced products and services, and any agreements with state and non-state entities;
6. Create, maintain, and enforce information security policies, standards, procedures, and guidelines;
7. Create secure configuration standards for hardware, software, and network devices, in compliance with state published standards, including the Email Threat Protection Standard (SIMM 5315-A);
8. Implement administrative, technical, and physical controls for the protection of information assets as part of the system engineering process; and
9. Share Threat Information, as defined in National Institute of Standards of Technology (NIST) Special Publication (SP) 800-150, with the California Department of Technology via direct electronic means.

Implementation Controls: [NIST SP 800-53: System and Services Acquisition \(SA\)](#), [Email Threat Protection Standard \(SIMM 5315-A\)](#), [NIST SP 800-150: Guide to Cyber Threat Information Sharing](#)