

**SAM – INFORMATION SECURITY**  
**(Office of Information Security)**

**PERSONNEL MANAGEMENT**  
(Revised 12/13)

**5305.4**

**Policy:** Each state entity must identify security and privacy roles and responsibilities for all personnel. This will ensure personnel are informed of their roles and responsibilities for using state entity information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include:

1. Employment history, fingerprinting, and/or criminal background checks on personnel who work with or have access to confidential, personal, or sensitive information or critical applications may be necessary for a particular state entity. Each state entity should consult the California Human Resources Department and the Department of Justice for specific rules and regulations relative to employment history, fingerprinting, or criminal background checks.
2. Initial training of state entity personnel with respect to individual, state entity, and statewide security and privacy responsibilities and policies before being granted access to information assets, and annually thereafter.
3. Signing of acknowledgments of security and privacy responsibility by all personnel.
4. Transfer procedures that ensure access rights and permissions to state entity information assets are reviewed for appropriateness and reauthorized by program management when personnel is transferred within the state entity, so that access to information assets is limited to that which is needed by personnel in the performance of their job-related duties.
5. Termination procedures that ensure state entity information assets are not accessible to separated personnel.