

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

AGENCY MANAGEMENT RESPONSIBILITIES

5315.1

(Revised 10/09)

Executive Management—The agency director has ultimate responsibility for information technology security, risk management, and privacy within the agency. Agency directors are responsible and shall take reasonable measures for implementation of, and compliance with, the state security policy and are accountable for the computerized information resources held by their agencies. Agency directors are responsible for the integrity of computerized information resources and the authorization of access to those resources. All agency employees share in this responsibility as well. On an annual basis the Director of each state agency must submit an Agency Designation Letter (SIMM Section 70A) designating critical personnel. See SAM Section 5360. Each year, the agency director must certify that the agency is in compliance with state policy governing information technology security, risk management, and privacy program by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). See SAM Sections 5305 and 5360. The Director must also transmit each year an updated copy of the agency's Disaster Recovery Plan with the Agency Disaster Recovery Plan Transmittal Letter (SIMM Section 70D), or Agency Disaster Recovery Plan Certification (SIMM Section 70B) to the Office. See SAM Sections 5355 and 5360.

Information Security Officer—Oversight responsibility at the agency level for ensuring the integrity and security of automated and paper files, databases, and computer systems must be vested in the agency Information Security Officer (ISO). The ISO is required to oversee agency compliance with policies and procedures regarding the security of information assets. The ISO must be directly responsible to the agency director for this purpose and be of a sufficiently high-level classification that he or she can execute the responsibilities of the office in an effective and independent manner. It is acceptable to create this reporting relationship on a functional basis rather than reorganize the department. To avoid conflicts of interest, the ISO (for agencies other than state data centers) should not have direct responsibility for information processing, technology operations, or for agency programs that employ confidential information.

Disaster Recovery Coordinator—Each agency must designate a Disaster Recovery Coordinator to represent the agency in the event of a disaster or other event resulting in the severe loss of IT systems capability. The designated individual must have sufficient knowledge of information management and information technology within the agency to work effectively with the data centers and vendors in re-establishing information processing and telecommunications services after an event has occurred. The name, title, business address, and phone number of the coordinator must be submitted to the Office with the agency's Disaster Recovery Plan, and annual Agency Designation Letter (SIMM Section 70A), as appropriate. See SAM Section 5360.

Technical Management—Agency information technology management is responsible for (1) implementing the necessary technical means to preserve the security, privacy, and integrity of the agency's information assets and manage the risks associated with those assets and (2) acting as a custodian of information per SAM Section 5320.3.

Program Management—Agency program managers are responsible (1) for specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) for ensuring that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.

The establishment of positions to meet agency information security responsibilities must be justified in accordance with established personnel and budgetary requirements.