

SAM – INFORMATION SECURITY
(Office of Information Security)

POLICY, STANDARDS, AND PROCEDURE MANAGEMENT

5310

(Revised 06/10)

The purpose of information security policy, standards, and procedures are to establish and maintain a standard of due care to prevent misuse or loss of state agency information assets. Policy provides management direction for information security to conform with business requirements, laws, and administrative policies. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy. And procedures are the specific series of actions that are taken in order to comply with policies and standards.

Each agency must provide for the integrity and security of its information assets by establishing appropriate internal policies, standards, and procedures for preserving the integrity and security of each automated, paper file, or data base including:

1. Establishes and maintains management and staff accountability for protection of agency information assets.
2. Ensure the use of social media technologies is in compliance with the Social Media Standard (SIMM 66B).
3. Establishes and maintains processes for the analysis of risks associated with agency information assets.
4. Establishes and maintains cost-effective risk management practices intended to preserve agency ability to meet state program objectives in the event of the unavailability, loss or misuse of information assets.
5. Agreements with state and non-state entities to cover, at a minimum, the following:
 - a. Appropriate levels of confidentiality for the data based on data classification (see SAM Section 5320.5).
 - b. Standards for transmission and storage of the data, if applicable.
 - c. Agreements to comply with all state policy and law regarding use of information resources and data.
 - d. Signed confidentiality statements.
 - e. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
 - f. Agreements to notify the state data owners promptly if a security incident involving the data occurs.
6. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:
 - a. Technology upgrade policy, which includes, but is not limited to operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
 - b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.
 - c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

(Continued)

SAM – INFORMATION SECURITY
(Office of Information Security)

(Continued)

POLICY, STANDARDS, AND PROCEDURE MANAGEMENT
(Revised 06/10)

5310 (Cont. 1)

- d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent, with the department's policy for making security upgrades and security patches.
 - f. Software management and software licensing policy, which must address acquisition from reliable and safe sources, and must clearly state the department's policy about not using pirated or unlicensed software.
 - g. Ensure that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Business use of peer-to-peer technologies must be approved by the CIO and ISO.
7. Requiring that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and security which have been established for the original data file must be applied in the new environment.
8. Establishing policy requiring encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes. (See SAM Section 5345.2).