STATE ADMINISTRATIVE MANUAL

MANAGEMENT MEMO

NUMBER:
MM 06-12

SUBJECT:
PROTECTION OF INFORMATION ASSETS

DATE ISSUED:
SEPTEMBER 1, 2006

EXPIRES:
UNTIL RECINDED

REFERENCES: CALIFORNIA GOVERNMENT CODE 11019.9, CALIFORNIA CIVIL CODE 1798 (ET SEQ), AND SAM SECTIONS 4841 AND 4841.1 AND STATEWIDE INFORMATION MANAGEMENT MANUAL (SIMM) SECTION 70C

ISSUING AGENCY:
DEPARTMENT OF FINANCE

BACKGROUND AND PURPOSE

The California Constitution declares that all people have an inalienable right to pursue and obtain privacy, specifically, Article 1, Section 1 of the California Constitution states: *"All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."* Privacy rights are further reaffirmed and the protection of personal information is mandated in Civil Code section 1798.1.

In response to recent security breaches of personal, sensitive or confidential information, this Management Memo reminds all state agencies, departments, boards and commissions that each is required to have implemented an information privacy program (mandated by Government Code section 11019.9), including rules of conduct regarding personal information (mandated by Civil Code section 1798.20), a designated employee in charge of ensuring program compliance (mandated by Civil Code section 1798.22), and other guidelines, procedures, training, and compliance as outlined in the Information Practices Act (IPA) (Civil Code section 1798 et seq.) and the State Administrative Manual (SAM) (section 4840 et seq.).

POLICY

All state entities must be vigilant to protect personal, sensitive or confidential information from inappropriate or unauthorized access, use or disclosure, regardless of media type. Whether a state agency is the custodian or the owner of the information, all employees must ensure the security and integrity of that information. Individuals of non-government entities contracted by the state are also included under this mandate (per Civil Code section 1798.19). While the SAM and other existing guidelines and procedures have focused in recent years on the security of electronic information assets, this policy pertains to all information assets, including, but not limited to, electronic and paper. Per Government Code section 11019.9, each state department, board and commission must implement and maintain an information privacy program. Information privacy programs must include:

- Procedures for the protection of all personal, sensitive, and confidential information, regardless of media type. In this context, any unique information about an individual would fall under this policy. These procedures should also delineate the differences of staff who have a right to the information and those who have a need to know. As a reference, we include definitions from the SAM sections 4819.2 and 4841.3:
    - Confidential Information – Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (PRA) (Government Code section 6250 et seq.), or other applicable state or federal laws.

- Sensitive Information – Information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be public; typically, sensitive information includes agency records of financial transactions and regulatory actions.

- Personal Information – Information maintained by state agencies that identifies or describes an individual.

- Public Information – Information maintained by state agencies that is not exempt from disclosure under the PRA, or other applicable state or federal laws.

- Instructions, as defined by the State Information Security Office, for reporting information security incidents particularly for inappropriate or unauthorized access, use or disclosure of personal, sensitive or confidential information, whether the information asset is in paper or electronic form. Included should be a process that ensures appropriate disciplinary action is taken in the event of a breach of policy and/or procedure.

- Ongoing education and training, at least annually, for all employees and contractors who handle personal, sensitive or confidential information. This includes a certification of training completion and the employee's understanding of the consequences of violating departmental information privacy policies. Consequences are defined in Articles 9 and 10 of the IPA.

- Ongoing audit and evaluation process to ensure adherence to department information privacy program.

ROLES AND RESPONSIBILITIES

Agency Secretaries and Department Directors will ensure that programs are in place to fully protect all personal, sensitive or confidential information assets.

The IPA (Civil Code section 1798.22) and the SAM (section 4841.1) require all state agencies to have an Information Security Officer (ISO), who oversees agency compliance with policies, guidelines and procedures regarding the security and protection of all personal, sensitive and confidential information assets. Associated with this Management Memo, each Director will certify on an annual basis to the State Information Security Officer that privacy guidelines have been developed, that training and education programs exist and are conducted on an annual basis and that internal control evaluations are in place to ensure compliance with each agency's information privacy program.

IMPLEMENTATION, NEXT STEPS, AND CONTACT INFORMATION

Changes to the State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) will be forthcoming.

The Office of Privacy Protection and the State Information Security Office have previously articulated privacy and security principles for the state. All agencies, boards and commissions will use these principles as a guide for their individual policies and procedures.

Office of Privacy Protection (OPP)
The OPP advises government entities on policies and practices to ensure confidential information protection regardless of media type. The OPP website offers links to a variety of privacy topics including recommended practices for privacy notification procedures and links to specific state privacy legislation.
(916) 574-8180
http://www.privacy.ca.gov/

State Information Security Office
The State Information Security Office provides statewide direction and leadership in managing information security and risk management for the State's information assets, including establishing direction through policy and procedures, and promoting prevention, effective incident management, and compliance monitoring.
(916) 445-5239
http://www.dof.ca.gov/OTROS/SecurityProgram/SecurityProgram.asp

SIGNATURE

Original SAM Management Memo signed by Michael C. Genest, Director

_____

MICHAEL C. GENEST
Director
Department of Finance