BUDGET LETTER

	NUMBER: 05-08
SUBJECT: INFORMATION TECHNOLOGY SECURITY POLICY - CLASSIFICATION OF INFORMATION	**DATE ISSUED:** June 3, 2005
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTIONS 4841.2 - 4841.7, 4842.1, 4842.2, 4845, CALIFORNIA CIVIL CODE SECTION 1798.29, CALIFORNIA CIVIL CODE SECTION 56, CALIFORNIA HEALTH AND SAFETY CODE SECTIONS 123100 – 123149.5, FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, 45 C.F.R., PARTS 160 AND 164	**SUPERSEDES:**

TO: Agency Secretaries
Department Directors
Departmental Budget Officers
Departmental Chief Information Officers
Departmental Information Security Officers
Department of Finance Budget Staff

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your departments' Information Security Officers (ISOs) and departments' Chief Information Officers (CIOs). The Finance State ISO Office will also distribute this BL separately to the ISOs and CIOs on the current contact list.

BACKGROUND

The Department of Finance (Finance) is responsible for establishing the framework for the state's information technology (IT) security policies and activities, and for IT security oversight. This BL expands upon and clarifies policy about classification of information.

Data classification is part of each agency's Information Technology (IT) risk management program, as described in the State Administrative Manual (SAM) Sections 4841.2 and 4841.3.

The state's automated files and databases are essential public resources that must be protected from unauthorized use, access, disclosure, modification, loss, or deletion. Data classification is a key element to identifying appropriate levels of precautions to protect these resources.

In support of state and federal privacy protection laws, this BL modifies policy in SAM Section 4841.3, significantly expanding on existing classification criteria to be consistent with current laws.

When the word "agency" is used in the policy and within this BL, the meaning is consistent with the definition in SAM Section 4819.2: "When used lower case (agency), refers to any office, department, board, bureau, commission or other organizational entity within state government."

POLICY DESCRIPTION

Each agency is required to maintain the integrity and security of its automated information, per SAM Sections 4841.2 through 4841.7. Current policy for data classification requires extra precautions for confidential and sensitive information. The revised policy adds the definition of personal information, and the requirement to safeguard it appropriately. The revised policy also cites three state and federal laws protecting the privacy of personal information:

1. **Notice-triggering personal information**, which includes specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number), that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. This supports Civil Code Sections 1798.29 and 1798.3;
2. **Protected health information**, which is individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. This supports the state Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health and Records Act, Health and Safety Code 123100-123149.5; and
3. **Electronic health information**, which is individually identifiable health information transmitted by electronic media or maintained in electronic media. This supports the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R parts 160 and 164.

Data classification and the application of appropriate data safeguards are key components of effective risk management programs. Agencies are required to maintain risk management programs that include data security practices (SAM Section 4842.2.4), to conduct risk analyses on a regular basis (SAM Section 4842.1), and to provide annual Risk Management Certifications (SAM Section 4845). Each agency must now include personal information in the data classification portion of risk analysis and risk management. The due date for the next annual Risk Management Certification is January 31, 2006. The 2006 certifications must take into account your department's ability to safeguard and appropriately handle personal information as well as the other categories described in SAM Section 4841.3.

The policy included as Attachment I, is effective immediately. The changes will appear in a future revision of the SAM. Attachment I contains the entire text of SAM Section 4841.3, as revised by this BL.

CONTACTS AND QUESTIONS

You may call the State ISO Office at (916) 445-5239 if you have questions about this BL.

/s/ Veronica Chung-Ng

Veronica Chung-Ng
Program Budget Manager

Attachment

Advance Copy of Changes to State Administrative Manual Section 4841.3

4841.3 CLASSIFICATION OF INFORMATION

(Revised xx/05)

The state's automated files and databases are essential public resources that must be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion. Every agency must classify each file and database using the following classification structure:

1. Public Information – information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act(Government Code Sections 6250-6265) or other applicable state or federal laws; and
2. Confidential Information–information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Sensitive Information and Personal Information, as defined below, may occur in Public Information and/or Confidential Information. Files and databases containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When sensitive or personal information is contained in public records, care must be taken to protect it from inappropriate disclosure.

While the need for the agency to protect data from inappropriate disclosure is important, so is the need for the agency to take necessary action to preserve the integrity of the data. Agencies must develop and implement procedures for access, handling, and maintenance of personal and sensitive information.

1. Sensitive Information –information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.
2. Personal Information – information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request:

    a. Notice-triggering personal information – specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. See Civil Code Sections 1798.29 and 1798.3;

Advance Copy of Changes to State Administrative Manual Section 4841.3

b. Protected Health Information – individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State law requires special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5; and,

c. Electronic Health Information – individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164.

Subject to executive management review, the agency unit that is the designated owner of a file or database is responsible for making the determination as to whether that file or database should be classified as public, or confidential, and whether it contains personal, and/or sensitive data. The owner of the file or data base is responsible for defining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of the information. See SAM Section 4841.5.