BUDGET LETTER

NUMBER:	05-32
SUBJECT: INFORMATION TECHNOLOGY SECURITY POLICY - ENCRYPTION ON PORTABLE COMPUTING DEVICES	**DATE ISSUED:** November 14, 2005
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTIONS 4841.2 THROUGH 4841.7, CALIFORNIA CIVIL CODE SECTION 1798.29, 45 C.F.R. Section 160.103, BL 05-08	**SUPERSEDES:**

TO: Agency Secretaries
Department Directors
Departmental Budget Officers
Departmental Accounting 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).

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 introduces policy concerning the encryption of specific types of data on portable computing devices and portable electronic storage media. Attachment I contains the text of the new policy.

Theft of portable computing devices, such as laptop computers, is a problem in the state and in private industry. Theft and other loss of portable computing equipment can lead to compromise of confidential, sensitive, or personal data, which in turn can lead to privacy issues and costly follow-up activities.

California Civil Code 1798.29 requires that state departments disclose breaches in which electronically stored, unencrypted personal information may have been acquired. Section (e) of Civil Code 1798.29 is quoted below, and contains this law's definition of "personal information."

> (e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either name or the data elements are not encrypted:
> (1) Social security number.
> (2) Driver's license number or California Identification Card number.
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Federal statute for the Health Insurance Portability and Accountability Act (HIPAA) requires special handling of Protected Health Information, which is defined in 45 C.F.R Section 160.103.

For the purpose of this policy, and as described in State Administrative Manual (SAM) Section 4841.3, Protected Health Information is personal information and must be safeguarded accordingly.

State policy already requires that departments protect data and equipment, per SAM Section 4841.5. However, the state continues to experience situations in which confidential, sensitive, or personal data is compromised when an unencrypted electronic device is lost or stolen. The policy introduced in this BL requires encryption of state data that is confidential, sensitive, and personal when it is stored on portable computing devices (including, but not limited to, laptops and notebook computers) and/or portable electronic storage media (including CDs and thumb drives).

The policy applies to all portable computing devices or portable electronic storage media that contain state data, including equipment owned by employees, vendors, contractors, or researchers. Where state-owned confidential, sensitive, and/or personal data exists, it must not be allowed on any portable equipment or media that is not protected. The policy does not apply to mainframe and server tapes at this time, but may be revised at a future date to apply to these as well.

State policy for data classification is in SAM Section 4841.3, and defines confidential, sensitive, and personal information. It also discusses agency responsibilities for identifying what data fits into these categories. BL 05-08 released June 3, 2005, modified policy in SAM Section 4841.3, significantly expanding existing data classification criteria to be consistent with current laws. A copy of the revised SAM Section 4841.3 released with BL 05-08 is included in this BL as Attachment II.

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

Currently each agency is required to classify data and to maintain the integrity and security of its automated information, per SAM Sections 4841.2 through 4841.7.

This BL announces new policy in SAM Section 4841.2 that requires the following: portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must use encryption or equally strong measures to protect the data while it is being stored. An advance copy of the new policy incorporated into SAM Section 4841.2 is included as Attachment I.

Not all portable computing devices or electronic storage media contain confidential, personal, or sensitive information. Only those that do contain this information require encryption under this policy. Departments/agencies should look at the results of their data classification efforts to determine which equipment and storage media must be encrypted.

To protect data and minimize the need for encryption, here are some ideas:

- Avoid storing confidential, personal, or sensitive information on laptops and portable devices.
- Classify your data and make sure you know what state data is on portable devices and storage media. This includes state data on employee-owned and vendor-owned devices and storage media.
- Portable computing devices are stolen more often than portable electronic storage media (CDs, thumb drives, and the like). If your agency must transport confidential, sensitive, or personal data for state business, consider putting it on encrypted electronic storage media instead of on the computing equipment, and carry the storage media separately.
- Minimize the number of confidential, sensitive, or personal records that are carried on portable devices; carry only what is essential for current business and remove data when its business use is over.

If you can't eliminate the need for encryption, here are some tips:

- When purchasing new laptops, notebooks, and other portable computing devices, be sure to include encryption software in the purchase if there is any chance that the equipment will eventually hold data that must be protected.
- If you must carry confidential, personal, or sensitive information, always encrypt it during storage.
- If encryption is not possible, use an equally effective measure to safeguard the data and have this solution approved in writing by the agency ISO.
- Please note that if your agency uses a department-approved equally effective measure, it may not be as strong as encryption. Please also note that the law currently cites encryption as the only technology that exempts departments from a privacy notification in the case of loss or theft of a device with protected information.

This policy is effective immediately and agencies must comply within four months after the publication of this BL. If your agency is not able to fully implement this policy by that time the agency must notify the State Information Security Office in writing and provide an expected compliance date.

CONTACTS AND QUESTIONS

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

/s/ Greg Rogers

Greg Rogers
Assistant Program Budget Manager

Attachments

Advance Copy of Changes to State Administrative Manual Section 4841.2

New policy appears in bold italics in subsection 2.e.7

4841.2 INFORMATION INTEGRITY AND SECURITY

(Revised xx/05)

Each agency must provide for the integrity and security of its information assets by:

1. Identifying all automated files and data bases for which the agency has ownership responsibility (see SAM Section 4841.4);

2. Ensuring that responsibility for each automated file or data base is defined with respect to:

    a. The designated owner of the information within the agency,

    b. Custodians of information, and

    c. Users of the information;

    d. Ensuring that each automated file or database is identified as to its information class (see SAM Section 4841.3) in accordance with law and administrative policy;

    e. Establishing appropriate policies and procedures for preserving the integrity and security of each automated file or data base including:

        1) Agreements with 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 4841.3);

            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) Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used; and

            f) Agreement to notify the State data owners promptly if a security incident involving the data occurs.

        2) Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information and information necessary for the support of agency critical applications.
        3) Auditing usage of dial-up communications and Internet access for security violations;

4) Periodically changing dial-up access telephone numbers;

5) Responding to losses, misuse, or improper dissemination of information;

6) 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.

7) 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.

For the purpose of this policy, the terms "confidential information" and "sensitive information" are defined in SAM Section 4841.3. For the purpose of this policy, "personal information" is defined in three categories in SAM 4841.3 as follows:

- ***notice-triggering information (Civil Code Section 1798.29),***
- ***protected health information (45 C.F.R. Section 160.103), and***
- ***electronic health information (45 C.F.R. Section 160.103).***

Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the agency ISO.

3. 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.

   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.

4. Each agency must establish policy to 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.

Each state data center must carry out these responsibilities for those automated files, databases, and computer systems for which it has ownership responsibility. See SAM Sections 4841.4 and 4841.5.

Oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems must be vested in the agency Information Security Officer.

The head of each agency is responsible for compliance with the policy in this section. See SAM Section 4841.

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;

    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.