| | |
|---|---|
| Office of Systems Integration "SERVING CALIFORNIA" | **ADMINISTRATIVE POLICY**<br>**Control Number: OSI-AP-06-09** |
| **Encryption on Portable Computing Devices** | **Effective Date: June 27, 2006** |

**Purpose**

The purpose of this policy is to establish encryption requirements for all portable devices that may contain State data that is confidential, sensitive or personal.

**Background**

Theft of portable computing devices, such as laptops, 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. The Office of Systems Integration (OSI), in accordance with direction from the Department of Finance, is establishing this policy to protect confidential, sensitive or personal data when it is stored on portable computing devices.

For purposes of this policy, "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.

Confidential and sensitive data are defined in the State Administrative Manual (SAM) Section 4841.3.

**Policy**

All 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.

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 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 you 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 Information Security Officer.
- Please note that if you use 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.

**Applicability**

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.

**References**

SAM Sections 4841.2 through 4841.7 and 4840, California Civil Code Section 1798.29, 45 C.F.R. Section 160.103, Department of Finance Budget Letters 05-32 and 05-08.

**Disclaimer**

The OSI technical staff may create supporting documentation to amplify the intent of this policy and to address requirements from governing entities or documents. State and/or Federal laws or guidelines can supersede this policy. Any exceptions to this policy must be approved by the OSI IT Manager.

**Exceptions**

There are no exceptions to this policy.

**Violations/ Enforcement**

Any known violations to this policy must be reported to the OSI IT Group. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with State rules. The OSI may advise law enforcement agencies when a criminal offense may have been committed.

**Approval**

**Original Signed by Christine Dunham** **6/27/06**

**CHRISTINE DUNHAM** **Date**
ACTING DIRECTOR
Office of Systems Integration