

	I n f o r m a t i o n S e c u r i t y P o l i c y
---	--

To: CDI Employees

No.: ISO-10

From: Information Security Office (ISO)

Issued: July 3, 2006

Subject: Device Encryption Policy

Expires: When Superseded

Policy

California Department of Insurance (CDI) requires that all employees, contractors and consultants who acquire or gather personal, confidential, or proprietary electronic information* during the course of performing their respective job duties on behalf of the CDI shall save such information on CDI network drives only.

If any CDI employee, contractor or a consultant requires electronic access to personal, confidential, or proprietary information while traveling or away from CDI office locations, the employee, contractor, or consultant will do so by connecting to the CDI network through a VPN provided by CDI using a CDI supplied laptop or tablet pc.

Any mobile computing device (i.e. laptop or tablet PC) or storage media (i.e. USB memory stick, CD, DVD, floppy disk, and portable/external hard drive) used by any CDI employee, contractor, or consultant to transmit, store or access personal, confidential, or proprietary information remotely must be equipped with the proper CDI standard encryption software without exception.

Purpose

To ensure that CDI personal, confidential and proprietary information is protected and not disseminated without proper approval or user knowledge.

* The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. The term confidential information means 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. The term proprietary information means any information, technical data or know-how in whatever form, including, but not limited to, documented information, machine readable or interpreted information, information contained in physical components mask works and art work, which are clearly identified and marked as being proprietary or otherwise restricted information.

A "mask work" is a "series of related images, however fixed or encoded - (A) having or representing the predetermined, three-dimensional pattern of metallic, insulating or semiconducting material present or removed from the layers of a semiconductor chip product; and (B) in which series the relation of the images to one another is that each image has the pattern of the surface of one form of the semiconductor chip product"

Procedure

The Information Technology Division (ITD) and ISO will maintain necessary procedures to secure and equip all CDI mobile computing devices used to transmit and store personal, confidential, or proprietary information; and, use encryption software to mitigate risks to CDI critical data and comply with state law. CDI staff, contractors and consultants are required to use only those mobile computing devices equipped with CDI approved encryption software to store, transmit or access CDI data remotely or when away from CDI office locations. Managers and supervisors will monitor and track employee(s) that use personal, confidential, critical or sensitive data on a regular basis and provide that list annually (January) to the ISO. Managers and supervisors should complete [ISO Form 002 \(Report of Employees who store, Personal, Confidential or Sensitive Data on mobile computing and or mobile storage devices on a regular Basis\)](#). The form is available on the department's intranet website [Forms](#) page.

Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3353 if you have any questions regarding this policy.