

CDI	Information Security Policy
------------	--

To: CDI Employees

No.: ISO-09

From: Information Security Office (ISO)

Issued: August 1, 2004

Subject: Physical Security Policy

Expires: When Superseded

Policy

California Department of Insurance (CDI) pursuant to ([SAM Section 5330 – Physical & Environmental Security Practices](#)), must control the physical access to information assets. This includes but is not limited to all CDI server rooms and telecom/switch closets. Only authorized CDI staff and vendors may access secure areas. ITD shall identify all secure areas and maintain a current listing of employees and/or vendors authorized to access these secure areas. Where applicable, key card access reports should be reviewed at least bi-monthly to discover unauthorized access attempts and entries. When an employee and/or vendor no longer needs access, ITD must ensure any access keys and keycards are returned to ITD immediately. CDI information assets must have fire prevention, detection, and suppression equipment as well as environmental damage control equipment installed in these secure areas. ITD must also have adequate power supply protection, detection, and monitoring in case of any loss to operational capabilities because of electrical power fluctuations or failures.

Purpose

To protect CDI information assets from unauthorized access and environmental hazards.

Inquiries

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

Archie Alimagno, Information Security Officer