



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.106	Physical Security	07/13/04

PURPOSE

To establish a countywide information security policy to ensure that County information technology resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

REFERENCE

Board of Supervisors Policy - Information Technology and Security Policy.

POLICY

Facility Security Plan

Each County department is required to have a "Facility Security Plan" which shall include measures to safeguard Information Technology resources. The plan shall describe ways in which all Information Technology resources shall be protected from physical tampering, damage, theft, or unauthorized physical access.

Proper Identification

Access to areas containing sensitive information must be physically restricted. All individuals in these areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

Access to Restricted IT Areas

Restricted I/T areas including data centers, computer rooms, telephone closets,

network router and hub rooms, voicemail system rooms, and similar areas containing I/T resources. All access to these areas must be authorized and restricted.

Equipment Control

The assigned user of I/T resource is considered the custodian for the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the involved department manager.

Sensitive I/T resources located in unsecured areas should be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

When feasible, I/T equipment must be marked with some form of identification that clearly indicates it is the property of the County of Los Angeles.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.