



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.101	Use of County Information Technology Resources	07/13/04

PURPOSE

To establish policies under which users (County employees, contractors, sub-contractors, volunteers and other governmental and private agency staff) may make use of County Information Technology resources.

REFERENCE

July 13, 2004, Board Order 10 -

Board of Supervisors Policy - Information Technology and Security Policy
Acceptable Use Agreement (Attached)

POLICY

County information technology resources are to be used for County business purposes.

County employees or other authorized user shall not share their unique (logon/system identifier) with any other person.

No user shall intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to County information technology resources. It is every user's duty to use the County's resources responsibly, professionally, ethically, and lawfully.

The County has the right to administer any and all aspects of County information access and use including the right to monitor Internet, e-mail and data access.

Monitoring/investigating employee access to County I/T resources (i.e., e-mail, Internet or employee generated data files) must be approved by department

management. If evidence of abuse is identified, notice must be provided to the Auditor-Controller's Office of County Investigations.

Users cannot expect the right to privacy in anything they create, store, send, or receive using County information technology resources.

All users of County information resources must sign an "Acceptable Use Agreement" prior to being granted access.

Definitions

County Information Technology Resources include but are not limited to the following:

Computers and any electronic device which stores and/or processes County data (for example: desktops, laptops, midrange, mainframes, PDAs, County wired or wireless networks, digital cameras, copiers, IP phones, faxes, pagers, related peripherals, etc.)

Storage media (diskettes, tapes, CDs, zip disk, DVD, etc.) on or off County premises.

Network connections (wired and wireless) and infrastructure, including jacks, wiring, switches, patch panels, hubs, routers, etc.

Data contained in County systems (databases, emails, documents repositories, web pages, etc.)

County purchased, licensed, or developed software.

Access Control

Unauthorized access to any County information technology resources, including the computer system, network, software application programs, data files, and restricted work areas and County facilities is prohibited.

Access control mechanisms must be in place to protect against unauthorized use, disclosure, modification, or destruction of resources.

Access control mechanisms may include hardware, software, storage media, policy and procedures, and physical security.

Authentication

Access to every County system shall have an appropriate user authentication mechanism based on the sensitivity and level of risk associated with the data.

All County data systems containing data that requires restricted access shall require user authentication before access is granted.

County information technology resource users shall not allow others to access a system while it is logged on under their user sessions. The only exceptions allowed are when the software cannot be configured to enforce a log-in, or where the business needs of the Department require an alternate login practice for specified functions.

Representing yourself as someone else, real or fictional, or sending information anonymously is prohibited unless specifically authorized by department management.

County information technology resource users shall be responsible for the integrity of the authentication mechanism granted to them. For example, users shall not share their passwords, electronic cards, biometric logons, secure ID cards and/or other authentication mechanisms with others.

Fixed passwords, which are used for most access authorization, must be changed at least every 90 days.

Data Integrity

County information technology users are responsible for maintaining the integrity of County data. They shall not knowingly or through negligence cause County data to be modified or corrupted in any way that compromises its accuracy or prevents authorized access to it.

Accessing County Technology Resources Remotely

Access to County technology resources by an employee or non-County employee owned equipment must be approved by department management and/or be part of an approved contract. In all cases, the equipment being used for access must be compliant with County security software requirements.

Privacy

Information that is accessed using County information technology resources must be used for County authorized purposes and must not be disclosed to others.

Confidentiality

Unless expressly authorized by department management or policy; sending, disclosing, or otherwise disseminating confidential data, protected information, or

other confidential information of the County is strictly prohibited. This includes information that is protected under HIPAA or any other privacy legislation.

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.