



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.109	Security Incident Reporting	05/08/07

PURPOSE

The intent of this policy is to ensure that County departments report information technology (IT) security incidents in a consistent manner to responsible County management to assist their decision and coordination process.

REFERENCE

Board of Supervisors [Policy No. 3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

May 8, 2007, [Board Order No. 26](#)

Board of Supervisors [Policy No. 6.100](#) – Information Technology and Security Policy

Board of Supervisors [Policy No. 6.101](#) – Use of County Information Technology Resources

Board of Supervisors [Policy No. 6.103](#) – Countywide Computer Security Threat Responses

Board of Supervisors [Policy No. 6.110](#) – Protection of Information on Portable Computing Devices

POLICY

All information technology (IT) related security incidents (i.e., virus/worm attacks, actual or suspected loss or disclosure of personal and/or confidential information, etc.) must be reported to the applicable designated County offices in a timely manner to minimize the

risk to the County, its employees and assets, and other persons/entities. The County department that receives a report of an incident must coordinate the information gathering and documenting process and collaborate with other affected departments to identify and implement a resolution or incident mitigation action (i.e., notification of unauthorized disclosure of personal and/or confidential information to the affected employee and/or other person/entity, etc.)

In all cases, IT related security incidents must be reported by the Chief Information Office (CIO) to the Board of Supervisors (Board) delineating the scope of the incident, impact, actions being taken and any action taken to prevent a further occurrence. Board notification must occur as soon as the incident is known. Subsequent updates to the Board may occur until the incident is closed as determined by the Chief Information Security Officer (CISO).

Each County department must coordinate with one or both of the designated County offices (CIO and the Auditor-Controller), as applicable, when an IT related security incident occurs. For purposes of this coordination, the CISO has the responsibility for the CIO. The County HIPAA Privacy Officer (HPO) and the Office of County Investigations (OCI) have respective responsibilities for the Auditor-Controller.

Chief Information Security Officer (CISO)

All IT related security incidents that may result in the disruption of business continuity or actual or suspected loss or disclosure of personal and/or confidential information must be reported to the applicable Departmental Information Security Officer (DISO) who will report to the CISO. Examples of these incidents include:

- Virus or worm outbreaks that infect at least ten (10) IT devices (i.e, desktop and laptop computers, personal digital assistants (PDA), etc.)
- Malicious attacks on IT networks
- Web page defacements
- Actual or suspected loss or disclosure of personal and/or confidential information
- Loss of County supplied portable computing devices (i.e., laptops, PDAs removable storage devices, etc.)

HIPAA Privacy Officer (HPO)

All IT related security incidents that may involve patient protected health information (PHI) must be reported by the affected County departments to the HPO. These incidents may be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- Compromise of patient information
- Actual or suspected loss or disclosure of patient information

Office of County Investigations (OCI)

All IT related security incidents that may involve non-compliance with any Acceptable Usage Agreement (Refer to Board of Supervisors Policy No. 6.101, Use of County Information Technology Resources) or the actual or suspected loss or disclosure of personal and/or confidential information must be reported to OCI. These incidents can be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- System breaches from internal or external sources
- Lost or stolen computers and data
- Inappropriate non-work related data which may include pornography, music, videos
- Actual or suspected loss or disclosure of personal and/or confidential information

Chief Information Office (CIO)

All IT related security incidents that affect multiple departments, create significant loss of productivity or result in the actual or suspected loss or disclosure of personal and/or confidential information shall be coordinated with the CIO/CISO. As soon as the pertinent facts are known, the incident will be reported by the CIO to the Board of Supervisors. The CISO shall be responsible for determining the facts related to the incident and updating the CIO and other affected persons/entities on a regular basis until the issue(s) are resolved as determined by the CIO and action(s) taken to prevent any further occurrence. A final report shall be developed by the CIO that describes the incident, cost of remediation and loss of productivity (where applicable), impact due to the actual or suspected loss or disclosure of personal and/or confidential information, and final actions taken to mitigate and prevent future occurrences of similar events.

Actual or suspected loss or disclosure of personal and/or confidential information must result in a notification to the affected persons/entities via a formal letter from the applicable County department describing types of sensitive/confidential information lost and recommended actions to be taken by the persons/entities to mitigate the potential misuse of their information.

Definition Reference

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

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.

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Sunset Review Date: May 8, 2011