6.109 - Security Incident Reporting
Effective Date: 05/08/07

PURPOSE

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

REFERENCE

May 8, 2007, Board Order No. 26 — Board of Supervisors — Information Security Policies

Board of Supervisors Policy No. 3.040 — General Records Retention and Protection of Records Containing Personal and Confidential Information

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, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement) , attached thereto

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

All County IT security incidents shall be reported by the Departmental Information Security Officer (DISO) to the Chief Information Security Officer (CISO), as required by County IT security policies, standards, and procedures, upon discovery to minimize the risk to the County, its employees and assets, and other persons/entities, and to ensure compliance with applicable laws, and to facilitate the prosecution of criminal acts against County IT resources.

The County Department that receives a report of a County IT security incident shall coordinate the information gathering and documenting process and collaborate with other affected County Departments to identify and implement a resolution or mitigation action (e.g., notification of unauthorized access, use, exposure, disclosure, and modification of personal information and/or confidential information to the affected employee and/or other person/entity).

The Chief Information Office shall immediately report to the Board of Supervisors (Board) County IT security incidents that involve unsecured confidential information or unsecured personal information, and other incidents as determined by the CISO.

Each County Department shall coordinate with one or both of the designated County offices (Chief Information Office and the Auditor-Controller), as applicable, when a County IT security incident occurs. For purposes of this coordination, the CISO has the responsibility for the Chief Information Office. The

Chief HIPAA Privacy Officer and the Office of County Investigations (OCI) have respective responsibilities for the Auditor-Controller.

Each County IT user is responsible for notifying the County Department's Help Desk and/or DISO as soon as a County IT security incident is suspected.

Chief Information Security Officer (CISO)

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

- Virus or worm outbreaks that infect computing devices, or appear to be crafted to targeted individual user(s), department(s), resource or data;
- Malicious attacks on telecommunications;
- Web page defacements;
- Actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information;
- Denial of Service or Distributed Denial of Service attacks;
- Malicious use of web-based applications;
- Unauthorized privilege escalation use of administrator credentials.

Chief HIPAA Privacy Officer

All County IT security incidents that involve Protected Health Information (PHI) shall be reported by the affected County Departments to the Chief HIPAA Privacy Officer. These incidents may be reported using an on-line form found at fraud.lacounty.gov . Examples of these incidents include:

- Compromise of patient information
- Actual or suspected loss or use, exposure, disclosure, and modification of patient information

Office of County Investigations (OCI)

All County IT security incidents that may involve non-compliance with any Acceptable Use Agreement (refer to Board of Supervisors Policy No. 6.101 — Use of County Information Technology Resources) or the actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information shall be reported to OCI. These incidents can be reported using an on-line form found at fraud.lacounty.gov . Examples of these incidents include:

- System breaches from internal or external sources access and;
- Inappropriate non-work related information which may include, without limitation, music and videos to an extent that is not permitted by Board of Supervisors Policy No. 6.105 and pornography;
- Actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information.

Chief Information Officer (CIO)

All County IT security incidents that affect multiple County Departments create significant loss of productivity, or result in the actual or suspected loss or disclosure of personal information and/or

confidential information shall be coordinated with the CIO/CISO. As soon as the pertinent facts are known, the County IT security incident shall be reported by the CIO to the Board. The CISO shall be responsible for determining the facts related to the County IT security incident and updating the CIO and other affected persons/entities on a regular basis until all issues are resolved as determined by the CIO and all actions are taken to prevent any further occurrence. A final report shall be developed by the CIO that describes the incident, cost of remediation, loss of productivity (where applicable), impact due to the actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information, and final actions taken to mitigate and prevent future occurrences of similar incidents.

Actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information shall result in a notification to the affected persons/entities via a formal letter from the applicable County Department, including, at a minimum, a description of the types of personal information and/or confidential information lost or disclosed, recommended actions to be taken by the persons/entities to mitigate the potential misuse of their information, and any other information required by applicable laws. The timing and content of the notification letter shall be determined in consultation with the CISO.

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "telecommunications" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County IT security incident" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

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.

As used in this policy, the term "Protected Health Information" has the meaning given in 45 CFR Â§160.103.

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

There are no exceptions to this policy.

~~RESPONSIBLE DEPARTMENT~~

~~Chief Executive Office~~

~~DATE ISSUED/SUNSET DATE~~

~~Issue Date: May 8, 2007~~	~~Sunset Review Date: May 8, 2011~~
~~Issue Date: March 17, 2011~~	~~Sunset Review Date: May 8, 2015~~
~~Review Date: October 15, 2014~~	~~Sunset Review Date: December 31, 2014~~
~~Review Date: January 6, 2015~~	~~Sunset Review Date: December 31, 2018~~