

MANAGEMENT DIRECTIVE

INFORMATION TECHNOLOGY SECURITY INCIDENT REPORTING

Management Directive # 08-04

Date Issued: **02/21/08**

New Policy Release

Revision of Existing Procedural Guide dated

Revision Made: **NOTE:** Current Revisions are Highlighted

Cancels:

DEPARTMENTAL VALUES

The Department continues to focus on the three priority outcomes. We have identified improved safety for children, improved timelines to permanency. Timely permanence is achieved, with the first permanency option being reunification, followed by adoption and legal guardianship with a relative followed by legal guardianship with an unrelated caregiver.

APPLICABLE TO

This directive applies to all Department staff (County employees, contractors, sub-contractors, volunteers and other governmental and private agency staff) who make use of County and/or Department Information Technology Resources.

DEFINITIONS

A. Confidential Information

Any information that is sensitive, proprietary or personal to which access must be restricted and whose unauthorized disclosure could be harmful to a person, process or to an organization.

B. Personal Information

Any information that identifies or describes an individual including, but not limited to, his or her name, social security number, physical description, home address, telephone number, education, financial matters and medical or employment history.

C. Patient Protected Health Information

Patient Protected Health Information is information, including demographic data that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,

And that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

D. Computer Virus / Worm

A software program that may be loaded onto a computer, usually without the knowledge of the user, to cause unexpected damage to the computer and/or other information technology resources.

E. Business Continuity

The activities and procedures, with defined outcomes and deliverables, that make up the business of providing services to the county and public as outlined by the Department's mission and goals.

F. Department Information Technology Resources

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

- Computers and any electronic device which stores and/or process County data (for example: desktops, laptops, midrange, mainframes, PDAs, County wired or wireless networks, digital cameras, copiers, IP phones, faxes, pagers, related peripherals, etc.)
- Portable Media on or off Department premises
- Network connections (wired and wireless) and infrastructure, including jacks, wiring, switches, patch panels, hubs, routers, etc.
- Data contained in Department systems (databases, emails, documents, repositories, web pages, etc.)
- Department purchased, licensed, or developed software.

G. Portable Computing Device

Portable computing devices include without exception the following:

- Portable computers such as laptops and tablet computers
- Portable mobile devices such as personal digital assistants (PDA), digital cameras, phones, and pagers
- Portable storage media such as flash drives, USB thumb drives, diskettes, tapes, CDs, DVDs, and zip disks

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, loss of portable computing device, etc.) must be reported to the applicable Department management in a timely manner to minimize the risk to the County and Department, its employees and assets, and other persons/entities. When the Department reports an incident, it 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.)

As used in this directive, the term personal information or confidential information has the same meanings as set forth in Board of Supervisor Policy No. 3.040, General Retention and Protection of Records Containing Personal and Confidential Information.

Additionally, DCFS Case records and data are confidential pursuant to Welfare and Institution Code (WIC) Sections 827 and 10850. The Los Angeles County Juvenile Court policy on confidentiality sets forth the details of the Court's interpretation of these statutory requirements.

- A. All IT related security incidents must be reported to the Departmental Information Security Officer (DISO) within 30 minutes of occurrence and/or notification.
- B. The DISO must report all IT related security incidents to Department management, the county's Chief Information Security Officer (CISO) and/or the Office of County Investigations (Auditor-Controller) within 60 minutes of notification.
- C. All staff must immediately report to the Department's management and the Departmental Information Security Officer any actual or suspected incident in which confidential information is lost and/or disclosed to, or obtained by, any unauthorized person. Notification of the security incident must be made in the most prompt and expedient manner after the incident has been discovered.

- D. 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 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 within ten (10) days of the incident.
- E. All IT related security incidents that may result in the disruption of business continuity must be reported to the Departmental Information Security Officer who must report the incidents to the CISO. Examples of these incidents include:
- Virus or worm outbreaks that infect at least ten (10) IT devices (i.e., portable computing devices, desktop computers etc.)
 - Malicious attacks on Department IT networks
 - Loss of County and/or Department supplied portable computing devices (i.e., laptops, tablet computers, personal digital assistants, removable storage devices, etc.) See Management Directive XXXX, Use of Department Portable Computing Devices.
- F. All IT related security incidents that may involve patient protected health information must be reported to the county's Health Privacy Officer. These incidents may be reported to the DISO and via on-line using the form found at www.lacountyfraud.org. Examples of these incidents include:
- Compromise of patient information
 - Actual or suspected loss or disclosure of patient information
- G. All IT related security incidents that may involve non-compliance with any Acceptable Usage Agreements (Please see Management Directives XXXX, Use of Department Information Technology Resources; XXXX, E-mail Usage; and XXXX, Use of Department Portable Computing Devices) or the actual or suspected loss or disclosure of personal and/or confidential information must be reported to the DISO and on-line using the form found at www.lacountyfraud.org. The DISO must report these incidents to the Auditor-Controller Office of County Investigations (OCI). Examples of these incidents include:
- System breaches from internal or external sources
 - Inappropriate use of Department and or County IT resources
 - Inappropriate non-work related data/information which may include games, pornography, music, videos, etc.
 - Actual or suspected loss or disclosure of personal and/or confidential information

H. 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 contactors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

PROCEDURES

A. LOSS OR DISCLOSURE OF PERSONAL AND/OR CONFIDENTIAL INFORMATION

1. In the event a portable computer containing personal and/or confidential information is lost or stolen, notify your immediate supervisor as soon as possible. In addition, if the device is lost or stolen, file a police report as soon as possible. Obtain a copy of the police report and provide it to your Office Head and the Bureau of Information Services.

The supervisor or designated back up must notify their Office Head and the Bureau of Information Services immediately after notification by the employee. The supervisor or his/her designated back up is to open a Service Desk Ticket to report the loss at (562) 345-6789. If the supervisor or his/her designated backup is notified after normal business hours (7:00 AM – 6:00 PM), they are to report the loss to the Internal Services Department Help Desk at (562) 940-3335.

2. In the event portable media containing personal and/or confidential information is lost or stolen, notify your immediate supervisor or his/her designated backup as soon as possible. The notification must include what personal and/or confidential information was stored on the portable media that was lost or stolen.

The supervisor or his/her designated back up must notify their Office Head and the Bureau of Information Services immediately after notification by the employee. The supervisor or his/her designated back up is to open a Service Desk Ticket to report the loss at (562) 345-6789. If the supervisor or his/her designated back up is notified after normal business hours (7:00 AM – 6:00 PM), they are to report the loss to the Internal Services Department Help Desk at (562) 940-3335.

3. In both instances above, the IT Service Desk or the Internal Services Department Help Desk must notify the Departmental Information Security Officer immediately after notification.
4. Upon notification by the IT Service Desk or the Internal Services Department Help Desk, the DISO must immediately notify appropriate Department management, the county's Chief Information Security Officer (CISO) by completing the Computer Security Incident Report. The completed report is to be emailed to CISOnotify@cio.lacounty.gov and appropriate department management.

B. DISRUPTION OF BUSINESS CONTINUITY

1. Any staff who suspects or knows their assigned desktop computer, portable computer or portable media is infected with a virus or worm, is to immediately notify the IT Service Desk at (562) 345-6789. If the infection is severe enough to prevent use of the computer or device, also report the problem to your immediate supervisor or his/her designated back up and advise them that the problem has been reported to the IT Service Desk.
2. If the IT Service Desk receives reports of ten (10) or more computers being impacted with the same virus / worm activity, notification must immediately be sent to the Departmental Information Security Officer (DISO).
3. Upon notification, the DISO must immediately notify appropriate Department management and the county's Chief Information Security Officer (CISO) by completing the Computer Security Incident Report. The completed report is to be emailed to CISOnotify@cio.lacounty.gov and appropriate department management.
4. The DISO must then activate and direct the Department Computer Emergency Response Team (DCERT) to respond to the threat. The DISO will coordinate the efforts of DCERT in mitigating the threat with the County-wide Computer Emergency Response Team (CCERT) if CCERT is activated.

D. LOSS OR DISCLOSURE OF PATIENT PROTECTED HEALTH INFORMATION

1. In the event portable media containing patient protected health information is lost or stolen, notify your immediate supervisor or his/her designated back up as soon as possible. The notification must include what personal and/or confidential information was stored on the portable media that was lost or stolen.

The supervisor or his/her designated back up must notify their Office Head and the Bureau of Information Services immediately after notification by the employee. The supervisor or his/her designated back up is to open a Service Desk Ticket to report the loss at (562) 345-6789. If the supervisor or his/her designated back up is notified after normal business hours (7:00 AM – 6:00 PM), they are to report the loss to the Internal Services Department Help Desk at (562) 940-3335.

2. The IT Service Desk or Internal Services Department Help Desk must notify the Departmental Information Security Officer immediately after notification.
3. Upon notification by the IT Service Desk or Internal Services Department Help Desk, the DISO must immediately notify appropriate Department management, the county's Chief Information Security Officer (CISO) and the Auditor-Controller Office of County Investigations.

The CISO is notified by completing the Computer Security Incident Report. The completed report is to be emailed to CISOnotify@cio.lacounty.gov and appropriate department management.

E. NON-COMPLIANCE WITH DEPARTMENT USAGE AGREEMENTS

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, Management Directives 08-01, Use of Department Information Technology Resources, 08-02, Use of Department Email, and 08-03, Use of Department Portable Computing Devices) must be reported to the Auditor-Controller Office of County Investigations. These incidents can be reported using an on-line form found at www.lacountyfraud.org.

APPROVAL LEVELS

Section	Level	Approval
A.-D	None	

LINKS

Board of Supervisor Policy Manual <http://countypolicy.co.la.ca.us>

RELATED POLICIES

Board of Supervisor Policy 6.101, Use of County Information Technology Resources
Board of Supervisor Policy 6.103, Countywide Computer Security Threat Response
Board of Supervisor Policy 6.109, Security Incident Reporting
Management Directive 08-01, Use of Department Information Technology Resources
Management Directive 08-02, Use of Department Email
Management Directive 08-03, Use of Department Portable Computing Devices

FORM(S) REQUIRED/LOCATION

HARD COPY: Board of Supervisor Policy 6.109, Form CSIR version 01/31/08,
Computer Security Incident Report

This page intentionally blank

	Countywide Information Security Program	
	Department of Children & Family Services	
Report #	Computer Security Incident Report	Date
2008 – 00X		mm / dd / yyyy

In accordance with County policy # 6.109 Security Incident Reporting, a report must be filed with the County’s Chief Information Security Officer (CISO) when an IT related security incident occurs. The completed report may be emailed to CISOnotify@cio.lacounty.gov. The report must delineate the scope of the incident, impact, action(s) being taken and any action(s) taken to prevent a further occurrence.

Type of Incident

(Incident types are: Stolen/Lost, Intrusion/Hack, Web Defacement, System Misuse, Denial of Service, Spoofed IP Address, Unauthorized Probe/Scan, Unauthorized Electronic Monitoring, Malicious Code (virus, worm, etc.), and other.)

Date and Time when Incident was Identified / Discovered

Location of Incident

(Physical address including specific building location)

Who Identified / Reported the Incident

(Full Name, Job Title / Position, email address, and Phone number (e.g., work, cell, etc.))

Workforce Members Involved with the Incident and/or with the Response

(Full Name, Job Title / Position, email address, and Phone number (e.g., work, cell, etc.))

Brief Synopsis by the Departmental Information Security Officer (DISO)

(Narrative or chronology)

Date and Time of the Incident (If known)

Department Initial Response

Action(s) Taken to Prevent Further Occurrence

Action(s) Planned to Prevent Further Occurrence

Internal Services Department Service Center and/or Departmental Problem Ticket(s) #
(Countywide Computer Security Incident Hot-Line number is (562) 940-3335)

Was Personally Identifiable Information (Pii) (i.e., Confidential / Sensitive) involved?

Yes No Unknown

Was the device / information encrypted?

Yes No
 Unknown

Was a Law Enforcement Report taken?

Yes No Unknown Agency _____ Report # _____

Departmental Information Security Officer – Print Name (First and Last), Sign, Date and Time

Information Technology Manager (or designee) – Print Name (First and Last), Sign, Date and Time

Chief Information Officer (or designee) – Print Name (First and Last), Sign, Date and Time

CISO (or designee) – Print Name (First and Last), Sign, Date and Time (signature signifies receipt)