

MANAGEMENT DIRECTIVE
LEADER CITRIX SYSTEM

Management Directive #MD 09-10

Date Issued:	10/09/09
<input checked="" type="checkbox"/>	New Policy Release
<input type="checkbox"/>	Revision of Existing Management Directive
Revision Made:	
Cancels:	None

DEPARTMENTAL VALUES

The Department of Children and Family Services (DCFS) continues to focus on the three priority outcomes; improved safety for children, improved timelines to permanency and reduced reliance on out-of-home care.

APPLICABLE TO

This directive applies to all Department staff (County employees) that use the Department of Public Social Services' Eligibility, Automated Determination, Evaluation and Reporting (LEADER) System.

CONFIDENTIALITY POLICY

All Department staff (County employees) above that use LEADER are responsible for protecting participant's confidential information, as well as County information and data.

DCFS hereby acknowledges the right of privacy of all persons as to whom there exists any LEADER System data. DCFS shall protect, secure, and keep confidential all LEADER System data in compliance with all applicable federal, State, County, DCFS, DPSS, and local laws, rules, regulations, ordinances, guidelines, directives, policies and procedures, relating to confidentiality and information security (including any breach of the security of the LEADER System, such as any unauthorized acquisition of LEADER System data that compromises the security, confidentiality, or integrity of personal

information), including California Civil Code Section 1798.82 and California Welfare and Institutions Code Section 10850. Further, DCFS shall take all reasonable actions necessary or advisable to protect all LEADER System data in its possession, custody, or control from loss or damage by any cause, including fire, theft, or other catastrophe. In addition, if requested by DPSS Director, DCFS shall provide notification to all persons whose unencrypted personal information was, or is reasonably believed to have been, acquired by any unauthorized person, and the content, method, and timing of such notification shall be subject to the prior approval of DPSS Director.

DCFS shall inform all its managers, supervisors and employees providing services herein under of the confidentiality provision of this Management Directive.

DCFS shall ensure that all confidential documents/papers, as defined under State law (including, but not limited to, Welfare & Institutions Code Sections 10850, 17006) relating to this MOU must be destroyed and not put in trash containers when DCFS and DPSS dispose of these documents/papers. All documents/papers to be destroyed are to be placed in a locked or secured container/bin/box and labeled "Destruct" until they are destroyed. No confidential documents/papers are to be recycled.

DCFS shall not publish, disclose, permit or cause to be published or disclosed, or include in any way of their products, reports, the name, address, or any personally identifiable information (PII) concerning the condition or circumstances of any employee, client, applicant, or participant from whom, or about whom, information is obtained. PII includes any information that can be used to search for or identify individuals, or any information that can be used to access an individual's file, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper. Should a report be published using data provided by DPSS, DPSS retains the right to review and comment on all such reports prior to distribution.

PURPOSE

Revenue Enhancement (RE) eligibility workers and regional clerical staff may now directly access the Department of Public Social Services (DPSS) Los Angeles County Eligibility, Automated Determination, Evaluation and Reporting System (LEADER) in their family finding search functions to determine if children and families are known to DPSS. This DPSS computer system provides financial and eligibility determination functions for Los Angeles County's Cal-Works, Medi-Cal, Food Stamps, and other welfare benefit assistance programs. The system is used by Child Protection Hotline and Regional clerical staff and the Revenue Enhancement Division's Eligibility Workers.

Staff will be able to search for family composition information directly from the LEADER system for clients who may be receiving CalWORKs, Food Stamps, Medi-Cal, or other assistance benefits. The Single Index (SI) computer application is being replaced by access to LEADER. Staff will go directly into the LEADER system to find family information they used to search for using Single Index.

Access to DPSS' LEADER system will be via the DPSS' Citrix Intranet connection into the system. DCFS users will be limited to Read Only access with the exception of the Medi-Cal Only Eligibility Workers, who process Medi-Cal Only benefits for children. All Users will be required to complete Security Agreements outlining the confidentiality of public social services applicant and participant information contained within the LEADER system. All County employees using the LEADER system have a legal obligation to protect the confidential information.

Roll out of LEADER Citrix in DCFS will be from October 5, 2009, through November 30, 2009. Clerical Administrators (CAs) will serve as the Office Coordinators/Champions for the initial implementation of the LEADER system. Once initial rollout of the system is completed, County Office Administrators (COAs) will process new User ID's upon request.

PROCEDURE

A. WHEN: REQUESTING ACCESS TO LEADER Citrix

NOTE: Staff need a User ID and a Password to access LEADER Citrix.

Staff Responsibilities

1. Submit completed and signed LEADER System User ID Request, and LEADER System User Security Agreement forms to your Supervisor for approval and signature.
2. Once the paperwork is processed, you will receive a User ID and Password via e-mail from DPSS.

Supervisor Responsibilities

1. Supervisor will review their employees' forms for completeness and approval. Supervisor will sign the forms, give a copy of the approved forms to the employee, place copies in the employee's office personnel folder, and forward the original forms to the LEADER Coordinator/COA.
2. For Supervisor User ID and password, submit completed and signed LEADER System User ID Request and LEADER System User Security Agreement forms to your manager for approval and signatures and processing on to the LEADER Coordinator/COA.

LEADER Coordinator/COA Responsibilities

1. CA Coordinator/Champions will use approved *DCFS LEADER Citrix Users and Security* forms to compile a users list for each of their locations. Then, the list will be

forwarded to Business and Information Systems Division's IT Service Desk. The IT Service Desk will coordinate with DPSS on the issuance of the LEADER Citrix User ID's. CA Coordinator/Champions will review the forms for completeness and:

- a. **Email the DCFS Citrix & LEADER Users list to the DCFS IT Service Desk** at this address: ProblemManagement@dcfs.lacounty.gov
- b. **Mail the DCFS Citrix & LEADER Users list with the original User ID Request and Security Agreement forms to:**
DCFS Business and Information Systems (BIS) Division IT Service Desk

Attention: Jesse Peralta and Diane Reush, Analysts
12440 East Imperial Highway, 5th Floor, Room 501
Norwalk, California 90650 Phone – (562) 345-6789 Fax – (562) 807-2163

2. CA Coordinator/Champions and/or COAs will review User ID lists sent from DPSS to BIS every two months for validation of current User ID's. User ID's not used in a 60 day or two month period will be automatically deactivated by DPSS. If a User ID needs to be reinstated, the COA/Supervisor will call the DCFS IT Service Desk to request the reactivation of the User ID.

B. WHEN: ACCESSING LEADER

NOTE: You can ONLY access LEADER Citrix from your office computer.

Staff Responsibilities

1. Staff are to access the LEADER system upon receipt of referrals and/or requests from regional CSW's and others for validation of family composition, Medi-Cal eligibility, family finding and other tasks directly related to child welfare.

Staffs' assistance to CSWs is vital to providing quality social work practices and assuring children receive needed services to thrive under the Department's supervision.

Hours of Availability

- Monday through Friday 5:45 AM – 9:00 PM
- Saturday 5:45 am – 2:00 PM
- Sunday – LEADER system is not available
- Only Child Protection Hotline (CPH) and Emergency Response Command Post (ERCP) eligibility and clerical staff persons have LEADER access 24/7

C. WHEN: YOU HAVE A PROBLEM WITH LEADER CITRIX

1. DCFS IT Service Desk.
(562) 345-6789. Monday through Friday 7:00 AM to 6:00 PM
2. Internal Services Department (ISD) Customer Assistance Center (CAC).
(562) 940-3305. Monday through Friday 6:00 PM to 7:00 AM and weekends/holidays.

D. WHEN: YOU FORGET YOUR PASSWORD

NOTE: You have three (3) chances to enter your correct password. If you fail the third time, the system will lock you out. You will need to call the IT Service Desk to reset your password.

Staff Responsibilities

1. Call DCFS IT Service Desk – Monday through Friday 7 AM to 6 PM, at (562) 345-6789.

For after-hour help – Monday through Friday 6 PM to 7 AM and weekends/holidays. Call Internal Services Department (ISD) Customer Assistance Center (CAC) at (562) 940-3305.

2. Identify that you need to reset your LEADER Citrix password.

NOTE: In addition to LEADER Citrix, there are DCFS Citrix and State Citrix. Therefore, you must state clearly that you are calling to have your LEADER Citrix password reset.

3. You will receive your new password through DCFS e-mail within one hour.

E. WHEN: REGULARLY SCHEDULED PASSWORD CHANGE

Staff Responsibilities

NOTE: The system requires you to change your password every 60 calendar days. It will continue to remind you to change your password 14 days before the expiration date. If you fail to change your password within the 14 days, you will be locked out. You will need to call the DCFS IT Service Desk to reset your password.

1. Call DCFS IT Service Desk – Monday through Friday 7 AM to 6 PM, at (562) 345-6789.

For after-hours help – Monday through Friday 6 PM to 7 AM and weekends/holidays call Internal Services Department (ISD) Customer Assistance Center (CAC) at (562) 940-3305.

2. Identify that you need to reset your LEADER Citrix password.

STATUTES/REGULATIONS

California Civil Code Section 1798.92

California Welfare and Institution Code Sections 827 and 10850

LINKS

Board of Supervisor Policy Manual <http://countypolicy.co.la.ca.us>
California Code <http://www.leginfo.ca.gov/calaw.html>
DCFS Policy <http://lacdcfs.org/Policy/Hndbook%20CWS/default.htm>
Division 31 Regulations <http://www.cdss.ca.gov/ord/PG309.htm>
Title 22 Regulations <http://www.dss.cahwnet.gov/ord/PG295.htm>

RELATED POLICIES

Board of Supervisor Policy 3.040, General Records Retention and Protection of Records Containing Personal and Confidential Information

Board of Supervisor Policy 6.101, Use of County Information Technology Resources

Board of Supervisor Policy 6.109, Security Incident Reporting

Board of Supervisor Policy 6.110, Protection of Information on Portable Computing Devices

Management Directive 08-01, [Use of Department Information Technology Resources](#) issued on 10-14-2008.

Management Directive 08-03, [Use of Department Portable Computing Devices](#)

Management Directive 08-04, [Information Technology Security Incident Reporting](#)

Management Directive 09-06, LEADER System User Security

Procedural Guide 0500-501.30, [Disclosures of Health and Mental Health Information To and From County Departments Providing Services to a Child/Youth](#)

Procedural Guide 0500-507.10, [Confidentiality Protocols for Telecommuting, Users of Portable Computing Devices and Mobile Workers](#)

FORM(S) REQUIRED/LOCATION

LA Kids:

LEADER System User ID Request
LEADER System User Security Agreement

LEADER EMPLOYEE INFORMATION SHEET

OFFICE DCFS	PRINT ALL ENTRIES Fax or email to LEADER Manage Personnel Section	DATE COMPLETED
-----------------------	---	----------------

IP Address	Employee Number **	Gender (circle)** M F		Circle Disaster Responsibilities	
Last Name **	First Name **	MI	Suffix	Essential Standby	Backup None
Payroll Title					
Work Schedule 5/40 4/40 9/80		Circle RDO if 4/40 or 9/80 Monday Tuesday Wednesday Thursday Friday			Date of Next RDO if 4/40 or 9/80
Work Phone ()	Work Hours From To	Lunch Hour From To	If work schedule is 9/80, what are your Work Hours for the "short day"? From: To:		
If telecommute, Circle Day(s) of Week Monday Tuesday Wednesday Thursday Friday					

*Required for all LEADER Users (Required data elements marked with **)*

Shaded areas are not required for non-DPSS users

Section/Location	Unit, if any
Functional Title- CITRIX User	Supervisor Name**

Signatures needed for processing.

Employee Signature: _____

Supervisor/Section Head
Signature: _____ Date: _____

DPSS Central Manage Personnel Officer Signature: _____

Copies to:
Original- DPSS Manage Personnel Officer
Copy- Employee
Copy- Office Personnel Folder

MP5 (5-2009)

Input Date:

LEADER System
USER SECURITY AGREEMENT
(for Non-DPSS County Employees)

As an employee of the County of Los Angeles, you will have access to confidential public social services applicant and participant information contained within the LEADER System. All County employees using the LEADER System have a legal obligation to protect this confidential information.

It is the policy of the County of Los Angeles and the Department of Public Social Services (DPSS) that each County employee, whether permanent, temporary, part-time, contract, or in any other status, is individually responsible for the protection of all confidential applicant and participant information, as well as all County information, data, and information processing resources to which he or she has access by virtue of employment.

As a LEADER System user, I understand that my security responsibilities include, but are not limited to, the following:

1. All data displayed by the LEADER System are confidential and shall not be disclosed to any unauthorized person(s) or group(s). If in doubt, I will consult with my immediate supervisor or manager.
2. I am responsible for the secrecy of my password
3. My password must neither be written down nor told to anyone. If I know or suspect that my password is known by someone other than myself, I must immediately change my password, and notify my immediate supervisor or manager.
4. I may only use the LEADER System for those specific functions for which I am authorized. Personal, non-County business, and/or unauthorized use of the LEADER System are forbidden. This includes the use of the email component within the LEADER System.
5. I understand that it is illegal for me to knowingly access the LEADER System and add, delete, alter, damage, destroy, copy or otherwise use the system to defraud, deceive, extort, or control data for wrongful personal gain.
6. Only data that I believe to be correct may be entered into the LEADER System. I am not to enter any data which I know or believe to be incorrect. I must notify my immediately supervisor, and if necessary, my chain of command, if I am ever requested to knowingly enter incorrect data.
7. When I leave my LEADER System workstation, I will either lock the workstation or logoff the LEADER network.
8. I am not permitted to use my password to logon to the LEADER network to allow any other person to access the system.
9. I am not permitted to install any software into the LEADER System without specific written DPSS management authorization.
10. I am not permitted to copy any software or related documentation from the LEADER System without specific written DPSS management authorization.
11. I am not permitted to connect or disconnect any hardware or peripherals to or from the LEADER System without specific written DPSS management authorization.

12. Any suspected violation of this LEADER System User Security Agreement, and/or any misuse or non-compliance with the LEADER System operating standards and procedures, shall be reported immediately to my immediate supervisor or manager.

I have read and understand this entire LEADER System User Security Agreement and agree to abide by it. I recognize that my failure to fulfill these responsibilities, including the actions of anyone else using my password, could result in the abuse of County information resources and data, and that the County may hold me responsible for such abuse.

I further understand that any violation of this agreement may result in disciplinary action including discharge, civil liability, and/or criminal prosecution as provided by federal and State of California laws, and/or local ordinance.

Executed this _____ day of _____, _____, at _____, California.

PRINT OR TYPE EMPLOYEE'S NAME

PRINT OF TYPE SUPEVISOR'S NAME

EMPLOYEE'S SIGNATURE

SUPERVISOR'S SIGNATURE

EMPLOYEE'S TITLE

SUPERVISOR'S TITLE

EMPLOYEE NUMBER

DATE

EMPLOYEE'S DEPARTMENT

Distribution: Original to: Department of Public Social Services
LEADER Central Security Manager
9320 Telstar Avenue Suite 132
El Monte, California 91731
Copy to employee's Office Personnel Folder
Copy to employee

Rev. 03/05/2001