

MANAGEMENT DIRECTIVE

AUTOMATED PROVIDER PAYMENT SYSTEM (APPS WEB) AND APPS REPORT SYSTEM USER SECURITY

Management Directive #MD 14-03

Date Issued: **6/26/2014**

New Policy Release

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, contractors, sub-contractors, volunteers and other governmental, private agency staff, etc.) that use the Automated Provider Payment Web System (APPS Web).

USE OF COMPUTER HARDWARE AND CONFIDENTIALITY POLICY

The County considers its information technology resources and related data to be of significant value and employees must exercise considerable responsibility in its use. Therefore, employees are required to complete a registration form that includes a signature acknowledgement indicating that they understand and agree to the terms of the user agreement as follows:

- APPS Web access is provided to the employee to be used in completing County work responsibilities. Employee agrees to use APPS Web hardware, software, and data (the APPS Web environment) only for County management approved business.

- Employee agrees to maintain the confidentiality of the County's business and citizens' private data.
- Employee agrees not to subvert or bypass any security measure intended to control or restrict access to the APPS Web environment. For example, employee will not share their computer identification codes (log-in ID, computer access codes, account codes, IDs, etc.) or passwords.
- Employee understands that he/she is also subject to policies in Management Directives (MD) #08-01 (Use of Department Information Technology Resources) and 08-07 (Child Welfare Information Security) which is signed annually at the time of Performance Evaluation Review.
- Employee understands that failure to comply with any portion of this Agreement may result in disciplinary action including suspension, discharge, and civil and/or criminal penalties.

PURPOSE

The overall purpose of this MD is to ensure that all staff with access to the Department of Children and Family Services (DCFS) APPS Web and APPS Report System comply with Auditor-Controller's system security mandates and related County application/security policies. This directive outlines staff and management joint responsibilities for ensuring the timely deactivation of user accounts; ongoing review of access rights to ensure separation of duties; adherence to revised registration processes; and compliance to mandated quarterly review requirements established to ensure timely updates and appropriateness of user access rights and privileges.

Background

The APPS Web application implemented on September 26, 2011 is used to manage Foster Care, Kin-GAP, Adoption, Mental Health and Probation paid placements. This new web-enabled system provides a streamlined approach while maintaining the functionality, design and screen-flow of the APPS99 legacy application. As part of this effort, the DCFS Security Officer officially assumed support for the APPS Web application thereby establishing a formal, centralized process for resolving security and access related issues. Although former DCFS Revenue Enhancement Division (RED) security staff are no longer able to directly modify security profiles, designated RED security staff may be granted 'inquiry only' security access rights so that they may continue to review user security profiles for access status and appropriateness.

Effective August 31, 2012, BIS and the Internal Services Department (ISD) jointly implemented Single Sign On (SSO) to the APPS Web system. SSO, a user authentication solution, ensures the timely deactivation of user accounts by automatically restricting access to any user not listed in the ISD Active Directory. The SSO solution also simplifies the log in process by eliminating the need for multiple User IDs and passwords. Utilizing this time-saving mechanism, authorized users may now use their existing Internet/Hosted User ID ("e" plus employee number) and password to access the APPS Web system.

On January 28, 2013, the SSO solution was also applied to the APPS Report System. The SSO solution requires users to reset their passwords every 90 days and automatically deactivates user accounts after 90 days of inactivity. Therefore, users who only access the **APPS Report System** should log onto the APPS Web at least once a month in order to prevent mass lockouts.

Users

The primary APPS Web users are the RED Foster Care, Kin-GAP and Adoptions Assistance Program eligibility staff. Other Los Angeles County employees may obtain access to the APPS Web/APPS Report systems if their job duties justify the use of these systems. Users requesting access rights to these systems must complete a registration form and follow the instructions outlined below.

PROCEDURE

A. WHEN: REQUESTING APPS WEB/APPS REPORTS SYSTEM ACCESS OR CHANGES (UPDATE OR DELETE USER'S ACCESS RIGHTS)

All staff requesting access or updates to these applications will be required to complete a new registration form (for each individual incident) and obtain the designated supervisor's approval and signature.

Supervisors are responsible for ensuring that access rights are immediately deactivated any time a user no longer needs access to the systems due to a change in status (i.e., job duties, job transfer, termination, retirement, etc.). The designated Supervisor should submit a signed registration form to the DCFS Security Officer detailing the required revisions/deactivations.

- Obtain a copy of the new registration form available on LAKIDS in the Forms section and provide required information.
- The revised APPS Web registration form must include the employee's job title and a detailed explanation indicating why the employee's job duties justify access to the APPS Web and/or the APPS Report System. In order to facilitate the mandated Quarterly Review, RED staff Location Code should be **S9056** regardless of their physical office location. Non-RED staff and other LA County Department staff, should enter the **appropriate office location code** in the Location Code field (i.e., BIS = S0247, Adoptions = S0216, etc).
- DCFS Revenue Enhancement Division Staff should deliver the completed/signed registration forms to their local Security Officer for processing. The Revenue Enhancement local Security Officer will forward the original to the DCFS Security Officer. A copy of the signed form should be retained in the employee's Office

Personnel Folder and by the local Security Officer to facilitate the Quarterly User Access Review.

- DCFS Non-Revenue Enhancement Division and Other Los Angeles County Department Staff should deliver their completed registration form to their supervisor for review and approval. The employee's supervisor should mail the original signed registration form directly to the DCFS Security Officer at the address indicated below and a copy should be retained in the employee's Office Personnel Folder.

DCFS Security Officer Contact Information:

Attention: DCFS Security Officer
12440 East Imperial Highway, 5th Floor, Room 501
Norwalk, CA 90650
Phone: (562) 345-6775 or (562) 345-6776
Fax: (562) 807-2163

Note: To ensure that all registration forms are processed in an expedient manner, the completed APPS Web registration form may be faxed or scanned as a PDF file and e-mailed, and then followed up with the original mailed copy as mentioned above.

Users and/or their Supervisors will receive a confirmation e-mail indicating that the request has been processed and log-in instructions will be provided.

Staff Responsibilities

1. Submit the completed and signed APPS Web registration form, which includes user information, access level selection, and user security policy agreements to the designated Supervisor for review and approval.
2. Once the paperwork is processed, the employee will receive an e-mail indicating that their APPS registration has been processed.

Supervisor Responsibilities

1. Each employee's supervisor will review and approve the registration form for access appropriateness.
2. Supervisors are required to review each employee's registration form for completeness, accuracy and appropriateness.

DCFS Revenue Enhancement Division Staff Supervisor Responsibilities

- a) Upon approval, the Supervisor will give a copy of the approved form to the employee, place a copy of the approved form in the employee's office

personnel folder, and forward the original to the designated local Security Officer.

- b) The Revenue Enhancement local Security Officer will forward the original registration form to the DCFS Security Officer and retain a copy to facilitate the Quarterly User Access Review for RED staff (S9056).

DCFS Non-Revenue Enhancement Division and Other Los Angeles County Department Staff Supervisor Responsibilities

- a) Upon approval, the Supervisor will give a copy of the approved form to the employee, place a copy of the approved form in the employee's office personnel folder, and forward the original to the DCFS Security Officer.

DCFS Security Officer Responsibilities

1. Receive and process APPS Web registration forms;
2. Verify that all required fields are complete/valid; if not, the Security Officer staff will contact the Supervisor for corrective action;
3. Ensure that only signed faxed/PDF e-mailed or original copies are processed;

NOTE: All faxed and PDF e-mailed copies are to be followed up with the signed original to the DCFS Security Officer.

4. Contact supervisors that have not followed up with a signed original delivery;
5. Disable the user account for non-compliance, as appropriate.

B. WHEN: CONDUCTING QUARTERLY REVIEWS OF ALL APPS WEB/APPS REPORT SYSTEM USER PROFILES

DCFS Department Responsibilities

The Auditor-Controller requires that DCFS conduct quarterly reviews of all APPS Web user profiles to ensure access appropriateness and separation of duties.

- Business Information Systems (BIS) will publish the APPS User Security Access Review Report in the APPS Report System on a quarterly basis. To help facilitate the review process, the quarterly report will include all active users and will be sorted by Location Code, Last Name and First Name.
- RED is responsible for reviewing all RED staff profiles. RED staff are identified by the assigned Location Code S9056 in the APPS Web.

- BIS is responsible for reviewing BIS, Information Services Department (ISD) and Auditor staff profiles. Staff in this category are identified in the APPS Web by the assigned Location Code S0247.
- Internal Controls will review all other staff profiles. Internal Controls staff and all other County department staff should use their appropriate office location code (i.e., Adoptions = S0216).

The next quarterly review report is scheduled to be published in the APPS Report System on September 30, 2014, and every three months thereafter. All changes resulting from the review should be submitted using the established registration process above (see Section A above) and due by the 15th of the following month. For example, all changes resulting from the March 31st Quarterly Review are due by April 15th, all changes resulting from the June 30, 2014 Quarterly Review are due by July 15th and so forth.

B. WHEN: REQUESTING ACCESS TO THE APPS WEB/APPS REPORT SYSTEM

Staff Responsibilities

Los Angeles County employees may obtain access to the APPS Web and APPS Report System only if their job duties justify the use of these systems.

C. WHEN: EXPERIENCING A PROBLEM WITH THE APPS WEB/APPS REPORT SYSTEMS

1. For tracking purposes, open a ticket in the ISD Services Management System (SMS);
2. To access the System, open Internet Explorer and type <http://scenter.co.la.ca.us>;
3. Determine the ticket type:
 - a) Incident Ticket: Event which is not part of standard operation and causes a break requiring a fix.
 - b) ISD Service Request: A request for support, service, information, advice or documentation. These requests are also known as IMACs (install, move, add or change).
4. Select DCFS eCAPS group; and
5. Provide specific instructions and relevant information (i.e., cannot login, account locked, case/placement and vendor numbers, description of problem, required corrective action, etc.).

DCFS IT Service Desk.
(562) 345-6789, Monday through Friday, 7:00 a.m. to 6:00 p.m.

Internal Services Department Customer Assistance Center (ISD CAC).
(562) 940-3305, Monday through Friday, 6:00 p.m. to 7:00 a.m. and
weekends/holidays.

RELATED POLICIES

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

Management Directive #08-07, [Child Welfare Information Security](#)

For Your Information #11-19, [Implementation of the New Automated Provider
Payment System \(APPS\) IBM Web Application](#)

FORM(S) REQUIRED/LOCATION

[Automated Provider Payment System \(APPS\) Web and APPS Report System
Registration Form](#) Revised on 3-20-2013