

**CALSTARS SECURITY**  
(No.134 July 2014)

**3602**

Purpose / Use

To operate in CALSTARS, designated Departmental Accounting (DAO) staff must be provided with a CALSTARS user identification, which allows access to various system features throughout the agency terminals.

References:

SAM 8080.1

Forms / Related Documents:

CALSTARS 95  
CALSTARS ACCESS – Supervisors Form

Due Dates:

Upon notification from DAO Unit Supervisor for:

- Separated Employee
- New Employee
- Reassignment of Duties

**CALSTARS SECURITY**  
(No.134 July 2014)

**3602.1**

This section is an excerpt of the CALSTARS SECURITY SYSTEM, published by the Department of Finance in September of 2009. A copy of the entire CALSTARS SECURITY SYSTEM is kept in the DAO CALSTARS Security Officer's desk. The unit responsible for CALSTARS security is the DAO – Fund Accounting Unit. The primary staff person designated this responsibility is the Associate Information Systems Analyst (AISA). The alternates are the Associate Administrative Analyst – Accounting Systems (AAA - AS) and the Accounting Administrator II.

The DAO CALSTARS Security Officer, in conjunction with the DAO Unit supervisors, sets up the user's authority levels consistent with the user's assigned duties. In making this determination, consideration is given to the individual needs of the unit as well as the requirements of internal control/separation of duties, (SAM 8080.1).

## **SECURITY FEATURES**

**3602.2**

(No.134 July 2014)

CALSTARS contains both internal and external security control features.

### **INTERNAL – CAL FIRE - DAO**

Internal security features are controlled by the DAO CALSTARS operational support staff. These include the following features: (1) Terminal Security, (2) Organizational Code Security, (3) Password Control, (4) Automatic Revoke, and (5) Hidden Password.

### **EXTERNAL – DEPARTMENT OF FINANCE**

External security features are controlled primarily by the individual agencies and include the following features: (1) Segregation of Functions and (2) Terminal Locks.

Regardless of the number of security features built into a system, its success or failure depends largely upon the user's willingness to adhere to established procedures and practices.

### **SEGREGATION OF FUNCTIONS**

SAM 8080.1 defines duties of which no one person can perform more than one. This factor must be considered wherever possible when determining the level of authority that will be given to each user. These duties are:

1. Designing Systems
2. Programming
3. Maintaining records file and operating mechanized equipment
4. Initiating disbursement document
5. Approving disbursement document
6. Inputting disbursement information
7. Receiving and depositing remittances
8. Inputting receipts information
9. Controlling blank check stock
10. Reconciling input to output
11. Initiating or preparing invoices

### **TERMINAL LOCKS**

In view of the numerous security features that are readily available and easy to use, terminal locks are deemed to be a redundant feature and are not used at CAL FIRE.

## **CALSTARS SECURITY FORM, CALSTARS 95** (No.134 July 2014)

**3602.3**

Access to CALSTARS can be achieved by completing the security form CALSTARS 95 for each user. This form is completed and signed by the DAO CALSTARS Security Officer. The completed forms are entered into the CALSTARS Security Entry Screens by the DAO CALSTARS Security Officer.

Access to the CALSTARS 95 is controlled by the DAO CALSTARS Security Officer and is not available to general staff.

## **COMPLETION OF CALSTARS 95** (No.134 July 2014)

**3602.3.1**

The User ID is 7 characters in length. It must contain the 4 digits assigned to CAL FIRE followed by the user's first initial of his or her first, middle and last name. If there is no middle initial, use X. The 4 digits assigned to CAL FIRE are the following:

- CSFS – Department of Forestry (3540)
- CSRA – Resources Agency (0540)
- CSFW – Special Resources Programs (3110)

Passwords **MUST** be 8 characters in length, case sensitive, and **MUST** contain three of the following:

- Alphabetic uppercase letter
- Alphabetic lowercase letter
- National character (#,@,\$)
- Numeric number

## **DAO CALSTARS SECURITY OFFICER** (No.134 July 2014)

**3602.3.2**

The DAO CALSTARS Security Officer will complete the CALSTARS 95 form when the CALSTARS Access – Supervisors Form is received.

The CALSTARS Access – Supervisors Form is completed when the following conditions occur: (1) personnel turnover; (2) reassignment of personnel; and (3) a new system feature is added.

- Separated Employee - Upon notification from DAO Unit Supervisor, submit a CALSTARS 95 form to delete the user ID.

- New Employee – Upon notification from DAO Unit Supervisor, submit a CALSTARS 95 form to add a new user ID for a new employee.
- Reassignment of Duties – Upon notification from DAO Unit Supervisor, submit a CALSTARS 95 form to add, change, or delete the functional capabilities of a user ID based on a change in job assignment.
- When a New System Feature Is Added – The DAO CALSTARS Security Officer will determine the DAO Units affected.
  - The DAO Unit Supervisor will determine which users will need modification to their rights and notify the DAO CALSTARS Security Officer.
  - The DAO CALSTARS Security Officer will submit a CALSTARS 95 form to update the established user.

## **DAO UNIT SUPERVISOR**

**3602.3.3**

(No.134 July 2014)

The DAO Unit Supervisor will notify the DAO CALSTARS Security Officer, via a CALSTARS ACCESS – Supervisors Form (in the folder: \Accounting\Accounting Share\DAO Route Slips – Forms) when the following conditions occur: (1) personnel turnover; (2) reassignment of personnel; and (3) when a new system feature is added.

- Separated Employee – Notify DAO CALSTARS Security Officer to delete user ID.
- New Employee – Notify DAO CALSTARS Security Officer of the user's functions and access to CALSTARS. Include name, date of birth, and access code (mother's maiden name).
- Reassignment of Duties – Notify DAO CALSTARS Security Officer to add, change, or delete the functional capabilities of a user ID based on a change in job assignment.
- When a New System Feature Is Added – The DAO CALSTARS Security Officer will determine the DAO Units effected.
  - The DAO Unit Supervisor will determine which users will need modification to their rights and notify the DAO CALSTARS Security Officer.

## **ESTABLISHMENT AND MAINTENANCE OF THE PASSWORD**

**3602.4**

(No.134 July 2014)

Within two business days of the DAO Unit Supervisor submitting the CALSTARS ACCESS – Supervisors Form, the CALSTARS 95 requested changes will be effective. The new User ID will be established with a temporary password of “12345.” When the user signs into CALSTARS using “12345,” the user will be forced to select a new password.

Assigning or changing a password is done through a secondary screen, which contains an instructional message at the bottom. Users are prompted by the system with appropriate action steps throughout the entire set-up process.

## **PASSWORD LIFE SPAN**

**3602.5**

(No.134 July 2014)

Once a password is assigned, it is valid for a maximum period of 90 days. After this period, the system requires the user to assign a new password on his or her next attempt to log onto CALSTARS. A message will appear at the bottom of the CALSTARS RACF SIGNON SCREEN requesting the user to assign a new password before he or she can continue with the logon process.

If a new password has not been assigned within 90 days after the initial 90 days, the user ID is assumed to be inactive and will be revoked.

If a user’s password has been revoked for non-use after 90 days, the user should send an email to the DAO CALSTARS Security Officer to re-set a password. The request should include the User ID name and access code.

- The DAO CALSTARS Security Officer must verify the user and reset the user’s password.
- The reset password will be established with a temporary password of “12345” When the user signs into CALSTARS using “12345,” the user will be forced to assign a new password.

If a user suspects that the user password is accessible by others, the user may change password right away and not wait for the 90 day cycle to end.

## **CALSTARS SECURITY REPORT (CSB017-1)**

**3602.6**

(No.134 July 2014)

The CSB017-1 is a listing of all active CALSTARS users within the agency, showing the different levels of authority established for each user. The DAO CALSTARS Security Officer can obtain a copy of this report quarterly or whenever a substantial update is done.

When received, review the listing and make any corrections. If necessary, contact the unit supervisor for updates to staff.

[\(see next section\)](#)

[\(see HB Table of Contents\)](#)

[\(see Forms or Forms Samples\)](#)