Table of Contents

Introduction: RACF data security guidelines

What RACF means

RACF (Resource Access Control Facility) is an IBM-licensed data security product installed by the Department of Human Services (DHS) Office of Information Services (OIS) staff and administered by each DHS agency. RACF protects data by granting or denying access to transactions using a unique CESN password for each user. **This password is the only security measure that prevents unauthorized access to our confidential information or changes to our data. Passwords should never be in a macro for security reasons.**

RACF protects data from accidental or unauthorized disclosure, data changes, or destruction by permitting access to only authorized users. Access by authorized users is accomplished through a CESN logon process using a unique assigned Userid and an individually selected password. RACF has the capacity to track which Userids and passwords are used to obtain or alter data.

Persons without a RACF Userid are not entitled to access, view, receive, or alter information protected by RACF. It is the responsibility of all authorized users to protect confidential client data in all forms electronic, written and verbal. This protection includes maintaining password secrecy, not sharing terminal access with others, and taking a proactive approach in the protection of client data and confidentiality.

What RACF accomplishes:

- Helps maintain confidentiality requirements;
- RACF eliminates unauthorized access to our client information to the extent that all staff protects their passwords from unauthorized individuals;
- Provides a data security tool;
- Provides the means to prohibit “browsing” by unauthorized individuals;
- New data screens and/or User Groups are created for special groups that allow access to needed data. Unauthorized users are not to “browse” through APD screens they do not need.

How RACF works

RACF is a complicated system made easier for sub-administrators to deal with by using shortcuts. It would be extremely difficult to attach each user to each transaction needed to do the work. RACF eliminates this problem by permitting a few or many related transactions into a Resource Profile. User Groups are created and given permission to access one or more Resource Profiles. Staffs with common needs are connected to an appropriate User Group. If a transaction changes or if a staff member changes, there is one simple add or delete action rather than hundreds.

Resource Profiles are created by grouping transactions (screens) with common use. Resource Profiles may consist of a single transaction or a large number of transactions. See the APD RACF General Resource Profiles and the Other Agency Access to APD Transactions sections.

Data in each Resource Profile "belongs to" or is the responsibility of a **Data Steward.** The Data Steward has the responsibility to determine what information is confidential and what user groups are "qualified" to have access to the information each transaction contains.

Individuals who need access to data are placed in a **User Group** with all other users who need the identical information. User Groups are then permitted access to Resource Profiles, based on a "need to know" basis. An individual may be in one or several User Groups.

The RACF **User Profile** contains unique identifying information about each user who needs access to information. Identifying information such as name, cost code, agency, social security number, and the User Group(s) the person belongs to are kept in the User Profile. This information is viewed/added/deleted through the RACF transaction. Every user must have a unique RACF Userid and use a *SECRET* password.

The branch manager will select an employee in each branch to be the **RACF Sub-Administrator**. If an individual is requesting access to APD data and it is approved by the manager, the Sub-Administrator can then add the rights to the individual.

RACF identifies users and authorizes access to protected data, and logs unauthorized attempts to enter the system and access to protected data. Reports can be generated providing specific information on User IDs that read, change, or delete information.

- ***Personal liability for unauthorized activity is based on the Userid number and password used for unauthorized activity. Protecting the secrecy of an individual's password is extremely important.***

Staff roles in relation to RACF

Definition and responsibilities
RACF Administrator

- Defined - The RACF Administrator, who works in the DHS Office of Information Services (OIS), is responsible for the technical aspects of maintaining the RACF security system.
- Responsibilities
  - Works with DHS and APD staff to ensure the system has been implemented efficiently and is maintained in sound working order.
  - Assists DHS agency RACF Data Steward with any technical issues they have in regard to the technical application of the RACF process.
  - Is responsible for all transactions created and maintained by OIS for APD are secured by the RACF Data Security Program.

Data Owner

- Defined - The Data Owner is responsible for making and communicating decisions with regard to the use, identification, classification and protection of specific data or transactions. There may be separate Data Owners for each system (e.g., Client Maintenance, Payroll, Inventory, Oregon ACCESS, etc.).
- Responsibilities
  - Consulted when Resource Profiles and User Groups are formed to ensure that the access requirements are accurate and fully describe who may receive information.
  - Consulted by Chief Data Steward to clarify access questions.

Chief Data Steward

- Defined - A central office position responsible for the authorization of access to APD and DHS data, based on qualification criteria.
- Responsibilities
  - Acts as liaison between the Data Owner and any Sub-Administrator or organization inquiring about access to data, or needing assistance with current data access.
  - Create resource profiles and user groups.
  - Deals with authorization for access to the RACF program.
  - All requests for access to data from non-APD organizations must be submitted to the Chief Data Steward.

Local Sub-Administrator

- Defined - The local Sub-Administrator has been given the responsibility of managing the local RACF process for their section or branch. The team usually consists of a manager and clerical support person with a back-up support person.
- Responsibilities
  - The manager:
    - Approves access to data for local APD staff.
    - Monitors security compliance of RACF users, groups assigned and users revoked by reviewing the report (WTS0365RA) that is received by each branch monthly.
    - Develops processes for maintaining RACF User Profile accuracy.
    - Emails or faxes the Chief Data Steward an IUP form 784 to add or delete a RACF Sub-Administrator.
  - The local Sub-Administrator:
    - Assists the manager by creating and maintaining the RACF User Profile for all staff members.
    - Adds, alters or revokes users as staff change in the APD office. A close working relationship with the APD personnel staff is essential.
    - Assists manager in monitoring for security compliance and developing processes for maintaining RACF User Profile accuracy.
    - Maintains individuals' RACF User Profile by updating as

changes occur (such as name or office address changes) and entering appropriate comments as to staff position and status, job rotation, termination, etc.
    - Acts as primary liaison with the Chief Data Steward.

- The back-up Sub-Administrator:
    - Assists the primary Sub-Administrator with maintenance activities. A back-up person may be necessary to ensure that staff are not locked out of transactions necessary to their job when the local Sub-Administrator is out.
    - Working with individual users:
        - Newly hired employees should be issued a Userid and password.
        - Employees who transfer in should be connected to the appropriate User Groups as necessary. Address, branch number and printer ID should be updated. Delete User Groups not needed.
        - Employees who transfer out should have User Groups removed if not needed at the new site. Do not revoke if they will be reporting to a new APD branch the following week.
        - Employees who change tasks should have the Manager determine which user groups are needed and if a change in access is required. The Sub-administrator should make the appropriate updates.
        - Employees returning to APD should not have a new Userid issued if they have ever had one in the past. Their RACF Profile still exists. Check the RACF system by their ID (if known) or by their name. Make necessary changes to their RACF Profile when it comes up. Change their password to their ID, resume, and instruct them to enter a new password. Note that some employees have been removed from the active RACF database and cannot be found in CICS RACF. These employees can be returned by the Chief Data Steward.
        - When resuming revoked users/changing passwords, the Sub-administrator must know the APD Userid requesting to be resumed or have their passwords changed. The Chief Data Steward will request information to resume unknown users.

Individual Staff Members (Users)

- Comply with agency security policies.
- Protect confidential client data.
- Protect their passwords by not sharing, loaning, or posting.
- Protect any security codes needed for updating certain transactions.
- Protect agency data processing equipment.
- Promptly report any violations observed to the local Sub-administrator. APD staff members are directed to follow procedures described in the APD Employee Handbook as well as other instructions in policy or worker guides.

Monitoring

RACF supports an array of report formats, including monitoring Userids making unauthorized attempts to get into transactions and which terminal they are using. This data is available for any audit or investigation purposes. Audits of individual worker activity may be requested through the Chief Data Steward.

- Management responsibilities
  Protection of confidential or sensitive information is the responsibility of all agency staff. Management has the added responsibility of ensuring that all staff are aware of and abide by established guidelines. Management attention to the agency security program is vital to its success.

- Sub-Administrator responsibility
  - Maintain data security in the local office by:
    - Ensuring the RACF Profile for office staff is kept current, including revoking Userids for staff no longer authorized;
    - Ensuring that the authority extended to RACF sub-administrators is not abused or misused;
    - Ensuring users are aware of confidentiality standards;
    - Providing training or procedures as necessary to meet agency standards.

Local Sub-administrator Actions

Revoking Employees

- Users no longer needing access are to have their RACF ID revoked and

terminated immediately.

New Employees

- Issue each new APD employee a RACF Userid.
- Make the appropriate User Group connections that the manager has approved.
- Instruct the new employee how to use their ID and password to logon to the mainframe.

Transferred Employees

- Transferring employees, staff re-hires, or users changing from a volunteer, work experience, part-time, or temporary status retain their **original** RACF Userid.
- When an employee is leaving the Sub-administrator is to remove all User Group connections that the employee may not need in the new branch or assignment.
- The gaining Sub-administrator is to connect the user to User Groups needed for duties of the new position.
- Contact the Chief Data Steward when a user changes branches to have the USEC security portion of the RACF Profile changed.
- Users should not be revoked when transferring from one APD position/location to another.

Change of Tasks (permanent or temporary)

- Managers authorize changes in an employee's tasks that require different access.
- Enter the information into the RACF Profile and make any necessary User Group connections and removals.
- Notify employee that access has been established.

Temporary Employee Absence

- Revoke the user's access if on extended leave.
- Note in the Comment Section why the person is revoked, i.e., medical leave, vacation, etc.
- Resume the user when they return from leave.

Employee Termination

- Immediately revoke users who leave APD employment.

- Enter the date in the Revoked date field (this will always show as today's date).
- Enter the date in the Terminated date field (this will always remain the date entered).
- Note in the Comment section why the user is revoked, i.e., took job elsewhere, retired, removed for cause, etc.

Returning Employees

- Look up the RACF ID or employee name for returning employees and resume their RACF profile.
- Do not issue a new RACF ID to an employee who worked for APD since 1994, when RACF was implemented.
- Employees whose RACF profile is not found can be resurrected by the Chief Data Steward if an ID existed at any time. RACF IDs are sometimes removed from the active database, but are never removed from the RACF system.

Special Access (Auditors, Private Contractors, etc.)

- State and federal auditors, private contractors or others who need temporary access to APD data receive that authorization from the Chief Data Steward. Any requests received in the field are to be forwarded to the Chief Data Steward.

Sub-Administrator Use of SDISTxx User Groups

Each Sub-Administrator has authority to connect users to their District group. Attaching the user to an SDISTxx (xx is the district number) User Group sets a table of branches for the User. For example, the SDIST12 table contains 0111, 1211, 3011, 3012, 3013, 3014, and 8210. SDIST12 contains all branches in District 12. The RACF Sub-Administrator must have management authorization to place a user in the User Groups SDISTxx. Connection to an SDISTxx group allows the user to use the PSET transaction to update cases in **any** of that district's branches. **It is never necessary to attach users to SDISTxx if they will not be updating case information in all district branches**. sub-administrators must be attached to SDISTxx themselves to be able to attach others to it. The Sub-Administrator uses Option 4, Connect User To Group, to assign the user. The user can still work cases in their "home" branch in a normal manner. If they need to work a case in another branch, they use the transaction PSET and change the branch number to the new cost center. This can be done as many times as necessary. Overnight, CICS changes the user's branch cost center back to the home branch automatically.

Remember to remove access to the SDISTxx you may have temporarily assigned to a "visiting" user. When the user returns "home" the user's Sub-Administrator does not have access to your SDISTxx group and will not be able to remove the user, and he/she can still update cases in any branch in your district.

Use of SDIST00 User Group

The User Group SDIST00 allows designated users to update cases anywhere in the state. Users connected to this group may use PSET to change to any branch and make necessary changes. Assignment to this User Group is permitted by the Chief Data Steward.

Profiles with a zero based branch field in their profile can be used as if statewide PSET access were assigned to a user.

PSET: Changing Branch Access or Printer ID

- Change branch cost center for purpose of updating cases.
  - The PSET transaction enables users to change their branch cost center to any branch in their district or statewide in order to **update** cases.
- PSET is not needed to read case data from any other branch.
- Management must authorize use.
  - Use of PSET must be authorized by management because it gives the user authority to create, update cases and issue benefits in every branch within the district.
  - When authorized, the local Sub-administrator connects a user to the appropriate SDISTxx group.
- Change printer ID.
  - A user can also change their printer ID using PSET. This enables them to print at any host printer in the branch or elsewhere. A host printer is one where a CICS program directs the printout.
  - Screen prints are not affected by RACF.

Using PSET to Customize a User Profile

The RACF Profile "Branch Number" defines which branch the user can update cases in and where the user will print transaction-based printouts.

If it is necessary to change printer ID or if the user wants to update cases from another branch within the user's district, the PSET transaction can temporarily change the RACF default settings. RACF changes the definitions back to the user's original branch and printer ID overnight.

To use the transaction, the person must be attached to the User Group "SDISTxx" with xx being the district number, and be signed on with a CESN Userid and password. At a clear screen, type PSET and press **{ENTER}**. The following screen appears:

```
DHR Printer/Branch Daily Re-Assignment Screen
Date: 05/23/2014
Time: 13:48

RACF User ID: HSxxxxx

Home Printer ID:          H1H6 New Printer ID: ????

Home Branch #:   0000 New Branch # : ????




Msg: You may enter a new printer/branch number
Msg: Press <ENTER> to process

F3=Exit
```

By entering a new printer ID or branch number in the appropriate field, users temporarily change their RACF file. This may be done any number of times daily.

If the wrong Printer ID is entered, PSET accepts it and sends data to be printer at the designated printer, even if the printer ID is invalid. Watch out for "O – oh" and "0 –

zero” errors.

PSET does not change printer IDs for SYSM or Screen Printing.

Users cannot change their branch number unless the local RACF Sub-Administrator has placed them in a special User Group (SDISTxx).

PSET NOTES:
PSET is only needed by APD staff that must change their branch ID before they can change case information in other branches. **PSET is not needed to read case data from other branches.** Staff must be management authorized to change other branch data before they are attached to a special district user group (SDISTxx). Each Sub-Administrator has the authority to connect the user to **their own district group.** For example, District 01 has SDIST01 access only. Connecting a user to SDIST01 allows that user to use the PSET transaction to change branch ID to any branch in District 01. If the user is temporarily stationed outside his/her home district, a Sub-Administrator can connect the user to the SDISTxx group where the user is working. When the user no longer needs to update cases in the temporary branch, the Sub-administrator in that branch must remove the user from the temporary SDISTxx group.

Passwords

User Password Management

- Passwords :
  - Are the personal responsibility of each person issued a RACF Userid.
  - Are to be secret and known only to the user. **sub-administrators must never ask a person for their password.**
  - Are the only "security wall" between the outside world (Internet) and our clients' personal data.
  - sub-administrators must make it clear to all staff that password protection is vital to data security and must not be taken lightly.
- Creating Passwords
  - When the user is first given a Userid, the default password is the Userid number. The first time the user encounters the CESN access screen, RACF asks for the RACF Userid and Password. When entered, RACF then asks for a new password. The user should be prepared to enter a password of their choice based on the DHS password policy criteria.

- ***It is a violation of security practices to create a "Macro" that enters the***

Userid and Password automatically.

Password Replacement

RACF requires a new password every sixty days. Users are notified by the addition of a third line on the "signon is successful" screen 14 days before their password expires. It looks like this:

CRTSNP : SIGNON IS COMPLETE
CRTSNP : THIS ACCESS DATE AND TIME IS 96012/10:39:04
CRTSNP : YOUR PASSWORD WILL EXPIRE IN 014 DAY(S)

The message counts down daily until a new password is created. If the user takes no action, on the last day the signon screen will cause the cursor to go to the "New Password" line. The user must enter a new password before proceeding any further. If the user does not create a new password at this point, the old password expires and future access attempts are denied. The RACF screens do not show a revoke date until the user tries to gain access.

A new password may be created any time a user signs on to CESN. The sign on menu asks for the user's Userid, Password and New Password. When a password is entered in the New Password entry line, it becomes the new password. The user must be cautious and type the password accurately as there is no "double-entry self-check." If an error is made, the user may never know what password he/she created. In that case, the Sub-Administrator needs to change it back to a default password (use the Userid) for the user to start over with.

Forgotten or Revoked Passwords

After five attempts to use an invalid or forgotten password, RACF returns the message "Supplied Password Incorrect" at the bottom left corner of the screen. On the sixth attempt with the wrong password, the RACF Userid is automatically revoked and the message "User ID is Revoked" appears at the bottom of the screen. At the seventh and any additional attempts, the message "User ID is Unknown to the ESM" appears. The user will not be able to gain access to any client information after the fifth wrong attempt. The Userid has been revoked on all sessions. No matter how many times the user tries, he/she will not gain access unless they are restored by a Sub-Administrator.

Users may have a problem with their password if an error is made on the first attempt by adding one character more than the true length of the password. Tabbing back and typing over the password does not delete that extra character and the password is still wrong. The User must tab back, use the “clear-to-end” process and then retype the password. If the password has been forgotten, the user will have to ask the Sub-Administrator to re-issue the default password. Menu Option 6, Change Password is used to issue a new default password. If revoked, the only way the user can regain access is to ask the Sub-Administrator to “Resume User”; Option 7 on the RACF Administration Screens. The screen shows a place to enter a date. By leaving it blank and pressing **{ENTER}**, the user is reinstated immediately.

The Sub-Administrator must be absolutely certain he/she is resuming the correct person. Do not resume users who have been terminated or intentionally revoked without verifying a change in circumstances that has made the user valid again.

Sign Off

To assure that non-authorized persons do not gain access to confidential or sensitive information, users must log off when leaving a terminal unattended or unprotected. After a specified period of inactivity, the terminal automatically signs off. This feature does not provide any protection for the period of time preceding the auto sign-off. You may sign off by typing “OFF” and pressing **{ENTER}** on a cleared screen. This takes the user back to the CICS Menu. Users must not sign off with “CESN” and leave the password menu on the screen. CESN is interactive with the mainframe and establishes a communication link. The mainframe sits and waits for the Userid and password, tying up space, making the mainframe run more slowly for other applications.

Do Not Create Macro's or Auto-Signons That Include a User Password

Automatic sign on processes that eliminate the user’s need to enter the password also eliminate the security provided by a password requirement. Management must take an active part in ensuring that these “shortcuts” are not being used. Macros that include a password are considered a violation of security.

RACF Reminders

Rules for Password Protection

No Posting - Do not write passwords down or hide them anywhere they can be found. This includes entering passwords into RACF or Oregon ACCESS while others can watch keystrokes. You are responsible for all actions taken under your password.

No Loaning - Do not lend your password to someone who has forgotten their own or who is going to need temporary access to data. Each person must access data through their own password, even if it is issued and revoked the same day.

No Sharing - Do not share passwords. This includes situations where staff may job share, temporarily help someone, or where there are only two people in a remote office. Each person must obtain and use their own private password.

No Macro's - An automatic sign on processes that eliminates your need to enter the password also eliminates the security provided by a password requirement. Macros that include a password are considered a violation of security.

CESN (RACF) Sign On and Sign Off Procedure

After receiving a Userid and default (temporary) password, staff may access the CICS system using the following CESN sign on procedure:

- Request access to CICS by entering a "G" (General Production), "T" (Test) or "W" (Training) on the menu screen. "G" is used by most staff.

- Clear the screen and type CESN and press the **{ENTER}** key. The password screen appears, asking for Userid, Password, Language and New Password.

- Type in the assigned Userid and default Password and press the **{ENTER}** key. ({**TAB**} between the Userid and Password.) *The first time a user signs on with CESN the default password will be the same as the Userid.* Ignore the Language entry line as it does not work. After entering the Userid and Default Password, the cursor moves to the New Password line and prompts for a New Password. A permanent "secret" password must be typed in by the staff person. Press **{ENTER}** to access CESN.

- Clear the “Sign on Successful” message from the screen. Notice there are two lines. In sixty days, when the password is about to expire, a third line will appear with a countdown to expiration. In that event, a new password can be selected and entered into the New Password line on the CESN signon screen. This is the only time a user is required to use the New Password line. Passwords used in the past may not be reused.

To log off : At a cleared screen, type “OFF” and press {ENTER} to exit and return to the main menu.

Standards for Creating RACF IDs for APD Users:

The following standards are used for all RACF IDs for APD users. Always check to see if the prospective user already has an ID. Check by ID, if known, **and** check by name. Persons who worked for APD from 1994 on will have an ID in the RACF database that, if not currently available, can be reinstated by the Chief Data Steward.

Establishing Chain of Accountability

- Each person must have an individual Userid.
- A chain of accountability can only be established if one identifiable user is assigned to one Userid.
- A Userid should never be shared with others.
- **Never** issue a Userid to a position such as “Guest User”, “Reception Desk”, “Temporary Clerk”, or “Volunteer.”
- Persons transferring to another APD office continue to use the same RACF ID.
- DO NOT RE-USE (recycle or re-issue) IDs to other users.
- DO NOT RE-ISSUE a new ID if a person has a name change. Use the same ID and just update the last name.
- Users terminating employment with the agency are to have their RACF (CESN) Userid immediately revoked. If the user returns later the same ID is to be used again.
- Do not create false Userids. The RACF data file must be kept free of data not directly related to a real user. We do not want any user to gain access to confidential information through false IDs that are forgotten.

- Userids created in error that have not been used can be deleted. Contact the Chief Data Steward.

Meaning of ID Characters

The Userid must be 7 characters long - no spaces or dashes. HSxxxxx

1) First Character
   H Designates a Human Resource user.

2) Second Character
   Identifier for the Division the User belongs to.

B=Health Div	R=OMAP
C=CSD (SCF)	S=APD
D=Director's Office	V=VRD
E=Employment	W=AFS
M=MHDDSD	Y=Oregon Youth Authority

3) Remaining Characters
   Unique identifying characters selected by each DHS agency. APD uses the three initials (TLP) of the employee and the last two characters are a numeric tiebreaker, (0 through 9).

Building a RACF User Profile

- The following steps are necessary to create an APD User Profile:
  - sub-administrators must know all transactions that are needed and which printer will be used.
  - The manager must review the request to see if it appears the requested access seems reasonable in relationship to the requestor's assigned duties. It is our intention that access be granted only on a "**need to know**" basis, while ensuring that all information needed to complete the work is available.

Determining Appropriate User Groups

- After all user Groups have been decided, a RACF ID can be assigned/created according to the Standards for Creating RACF IDs and a RACF profile built.

- Instruct the person how to use the RACF Userid and the default password. The Userid and password are issued to the person and the person is to change from the default password to the permanent one immediately.
- Give each new user a copy of RACF Reminders.
- Instruct the person regarding confidentiality and data security practices required by the agency.

RACF Administration Menus

The RACF Administration Menu - Items 1 through 8

1 - Add New User
   Displays a blank set of data entry screens used to add a new user to the RACF data set.

2 - Change Existing User
   Displays an existing user and allows existing data to be changed, corrected, RESUME, or REVOKE the user and narrate the reason at the same time.

3 - Display User
   Displays the data for the selected user but does not allow change.

4 - Connect User to Group
   Displays all User Groups the Sub-Administrator is delegated to attach staff to. Used to attach a user to specific group(s).

5 - Display/Remove User from Group
   Displays the groups a user is attached to. Used to delete the user from selected groups.

6 - Change User Password
   Used to reset the user password to a default password.

7 - Resume User
   Used to reactivate a revoked user.

8 - Revoke User
   Used to REVOKE (deny access to) the user. This may be invoked immediately or at a future date. (Option 2 is the preferred method so a narrative can be done at the same time.).

RACF Administration Menu

1 Add New User

2 Change Existing User

3 Display User

4 Connect User to Group

5 Display/Remove User from Group

6 Change User Password

7 Resume User

8 Revoke User

Enter Option --> Userid --> OR for options 2, 3, and 6
enter a name or partial name for a name lookup
Last Name First Name MI
_____ _____ ___

F1=Help F3=Exit Enter=Process

Main Menu

RACF Action Keys are shown at the bottom of the RACF screens.

F1 = Help	This function is not fully working yet. Some assistance is available for Menu Option items. (12/17/96).
F3 = Exit	Returns to the main menu **after** using **{ENTER}** to complete an action. If you are at the main menu, it exits from RACF. Using F3 **before** using the **{ENTER}** key prevents the record from being created or updated.
Enter = Process	Updates the RACF profile with the data that has been entered onto the screen. Also moves from one

screen to the next incomplete screen or back to the main menu.

ADD RACF USER

User ID: HS xxxxx Model after RACF ID: Division: SDSD

Last Name First Name MI EIN
_____ _____ _
_____

Address Line 1:
Address Line 2:
City: State: Zip Code: -_

Branch/Location: Employment Status:

Date - Assigned:

Comments:
_____

F1=Help F3=Cancel Enter=Process

Option 1 - Add New User

- Select a valid Userid for the new user.

- ALWAYS CHECK FOR PRIOR ASSIGNED USERIDS by both **name** and **ID**.
  - Use RACF menu option 3 to determine if the person has been issued a Userid in the past.
  - Enter the person's last name in the last name field for a list of users with that last name.
  - If the person has used another last name in the past, look for a Userid for that name also.

    - If they have had an ID in the past, check for that Userid.
- If neither the user's name nor ID can be found, and the user did have a RACF ID in the past, contact the Chief Data Steward. Periodically users who are not active are removed from the active RACF database. These IDs can be returned by the Chief Data Steward.
- Any ID that has been issued to a different user is not available. Assign/create a different RACF ID for the user you are building.
- To add (create) the new user, select Option 1 from the main RACF menu, enter the Userid you have selected and validated for the new user, and press **{ENTER}.** The **Add User** screen appears. The new Userid is in the upper left corner. If the new Userid is not what you wanted, press F3 to return to the main menu. This deletes the Userid and lets you start over.
- For a new Userid, you must use the "Model After" feature to create the USEC page. **If you fail to use a model for creating a new Userid, you must call the Chief Data Steward to have the USEC Security file (page 2) created.** Models can be selected from the monthly RACF User List report.
    - In the center of the first line of Option 1 is an entry cell labeled"Model after RACF ID". Enter the Userid of a person (a revoked ID will still model) that has the same duties as the user you are adding, then hit **{ENTER}**. This copies the modeled user's profile to the new Userid and fills in page 1 and page 2 of the RACF Profile. Correct the name, social security number and any other information on page 1. The model does not connect the new user to User Groups. RACF automatically takes you to Option 4, the list of groups, when creating a new user. Select the proper groups.
- Complete the RACF **Add User** screen as follows:
  These instructions are for both **Add User** (Option 1) and **Change User** (Option 2) choices on the RACF Administration Menu. Fill in the following screen fields. When done, press **{ENTER}** to save the data and to progress to the **Connect User** (Option 4) screen.

  Last Name Staff name **as shown on payroll records**
  First Name Staff name **as shown on payroll records**
  MI Middle Initial
  SSN Social Security Number or Employee ID number
  Address Line 1: Agency, branch
  Address Line 2: Street address, Suite, floor, room
  City: City, Town, or Village name

State: "OR"
Zip Code: i.e., 97310-1013 - all 9 characters (see HZIP)
Branch/Location: Branch/Section, Unit name

Employment status: **P** = Permanent APD staff
T = Temporary APD staff

Printer ID: Enter the terminal printer ID number primarily used.

Branch Number: Enter the user's 6 digit branch number (241800). The correct branch number must be entered in this field.

Revoke Date:

Terminated:

Comments: Use the comment line to indicate changes. Comments must be entered as to why a user is revoked at the time of termination. All comments should clarify the current status of the user.

- After entering all the above data items for a new user under Option 1, press **{ENTER}**. The screen moves to Option 4. **Connect User to Group.**

CHANGE RACF USER

User ID: HS xxxxx Division: SDSD

Last Name First Name MI EIN

_____ _____ __ _____

Address Line 1:
Address Line 2:
City: State: Zip Code: -

Branch/Location: Employment Status:

Date - Assigned: 05/30/2014 Revoked:// Terminated://

Comments:

F1=Help F3=Cancel Enter=Process

Option 2 - Change Existing User

To change the User Profile for an existing user, select Menu option 2, **Change User**. In the Option Box on the bottom of the Menu screen, enter **2** and the Userid **or** tab to the Last Name line and enter the name. The profile appears and you can make changes. If there is more than one user with the same name, a selection screen appears. By putting an "S" in front of the one you want and pressing **{ENTER}** that selected file will appear. Make any changes you need and press **{ENTER}** to update the record. Return to the menu **without** updating by pressing **{F3}**.

DISPLAY RACF USER

User ID: HS xxxxx Division: SDSD

Last Name First Name MI EIN
DOE JANE A 123456789

Address Line 1: 500 SUMMER ST
Address Line 2:
City: SALEM State: OR Zip Code: 97301 - 0000

Branch/Location: Employment Status: P

Date - Assigned: 05/30/2014 Revoked:// Terminated://

Comments:

F1=Help F3=Cancel Enter=Process

Option 3 - Display User

Menu item 3, **Display User** is used to look at a user profile. Access by entering **3** and the Userid in the Option boxes at the bottom of the menu. If you enter the Userid, information about the ID will be brought up. To conduct a Userid search, you may enter a portion of the Userid, the first 5 characters (HSTLP) for example, and all users with those first characters are listed on the screen. If you leave the Userid blank and enter part or the User's entire last name, an alpha search is made and all users with matching characters are listed on the screen. Placing any character in front of the user you wish to view and pressing **{ENTER}** displays that user. **{F3}** returns to the listing. This search process works in either Option 2 or Option 3. Press **{F3}** to return to the menu.

Connect User

Userid Default Group
HSxxxxx SHOLDGRP - HOLD GROUP USER AUTOMATICLY PUT HERE WHEN NEW ID

Position to:
__ SSUFIELD - SPD FIELD WORKER GROUP

F1=Help F3=Cancel F7=Page Backward F8=Page Forward Enter=Process

Option 4 - Connect Users to Group

The **Connect User to Group** menu item displays a list of User Groups. The groups look like the example above. To add a user to a group, move the cursor next to the group you want and type a character to select it, **"S"** for example. If additional groups are needed, move to the next group and repeat the selection process. Additional groups are accessed by paging down/up.

Press **{ENTER}** when all appropriate groups have been selected. A message at the bottom of the screen tells you if the action was successful.

Remove User

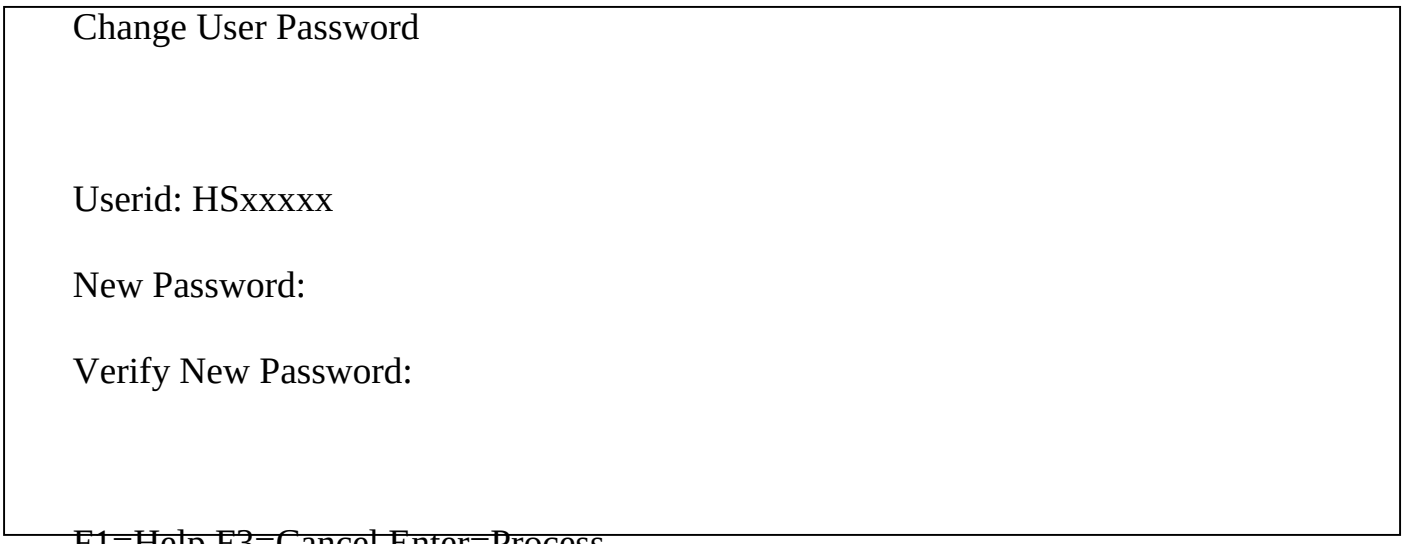
Userid Default Group
HSxxxxx SHOLDGRP - HOLD GROUP USER AUTOMATICLY PUT HERE WHEN NEW ID

__ SSUFIELD - SPD FIELD WORKER GROUP
__ SSUSSA - SPD SOCIAL SECURITY ADMINISTRATION

F1=Help F3=Cancel F8=Page Forward Enter=Process

Option 5 - Display/Remove User from Group

Use the **Display User/Remove User from Group** menu item to review a user to see what groups he/she is assigned to. You may also remove a user from a group by entering any character, **"S"** (select) for example; in front of the group name and pressing **{ENTER}.** Using option 5 you can remove users from groups they may have had in prior assignments. Please remove any groups that are not needed for a user's current assignment. If you see a blank line, that means the user belongs to a group that you, as a Sub-Administrator, do not have any authority over. Return to the menu without taking any action by pressing **{F3}**.



Option 6 - Change User Password

Use the **Change User Password** menu when the user forgets their password and you must reinstate it. The screen displays two lines, New Password and Verify New Password.

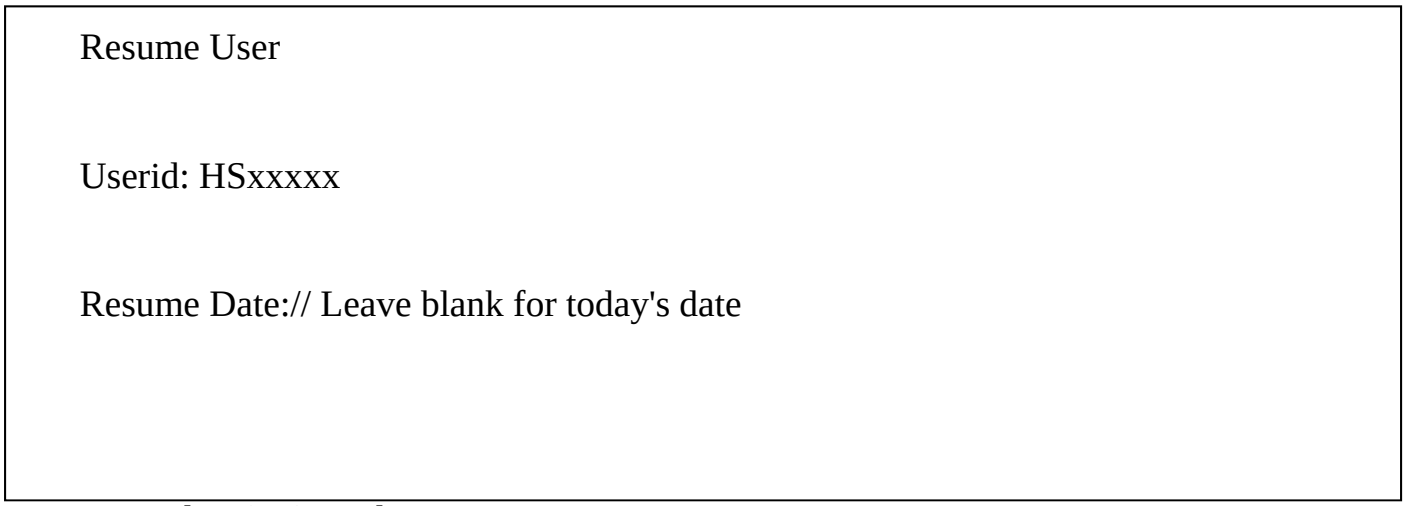
The new password is created as a temporary default password. It is used for one time only. To create a new password for a user, you may use the person's Userid or any easily remembered word as a default password, entering it on both lines; **{TAB}** from one line to the other. Press **{ENTER}** when done. The user uses the default password to validate the ID and create a new password.

Instruct the user to enter their ID on the ID line, the temporary password on the Password line, and to immediately go to the New Password line and create a new password. If the user presses **{ENTER}**, before creating a new password they will be able to get into CESN but for that one time only. The next time the user will be revoked.

RACF passwords expire after sixty days. Fourteen days before the expiration and every day thereafter, RACF notifies the user. The message appears as a third line on the successful signon message screen. If the user does not create a new password by using the **New Password** field during a signon process, the old one is revoked at the end of the 14 days. When that happens, the Sub-Administrator cannot use **Option 6**

Change Password by itself to get it to work again. You must first use **Option 7 Resume User**.
A user cannot re-use a password that was used in the past. RACF will not accept it. If the user attempts to, an invalid password message is displayed.

sub-administrators should not change passwords for users they do not know.



Option 7 - Resume User

The **Resume User** menu item displays a screen with a single line. Type in the **month/day/full year (all four digits)** you wish the user to be **Resumed** or restored, either the current or future date, never the past. Leaving the space blank makes the action immediate. Press **{ENTER}** to activate the action and **{F3}** to return to the menu. If the user was Revoked because of a password problem you may have to reset the password also.

You may also resume a user by using Option 2 and deleting the revoke date from the screen.
sub-administrators should not resume users they do not know.

It is a good idea to check the user's profile (Option 2 or 3) to see if there is any comment about why the user should not be resumed.

Revoke User

Userid: HSxxxxx

Revoke Date:// Leave blank for today's date

F1=Help F3=Cancel Enter=Process

Option 8 - Revoke User

The **Revoke User** menu item is used to prohibit access to any RACF protected data. The instructions are the same as for Resume User. Enter the date you want to Revoke, current or future; or leave blank to Revoke immediately. Pressing **{ENTER}** activates the command and **{F3}** returns to the menu. If Option 8 is used, the current or "today's date" always appears in the revoked line on the first page of the User Profile screens. **The preferred method is to use menu item 2, Change User and put the revoke date in the "Revoked:__/__/____" field.** At the same time you are Revoking the user, you must enter a terminated date and write narrative comments. Using Option 2 allows you to do both at the same time.

In the event that a user terminates employment from APD or no longer needs access to APD data, the user must be **immediately Revoked**. Also enter the termination date in the "Terminated:" field and narrate the reason in the "Comments:" field. This records the date and reason a user is being revoked and prevents someone else from restoring the user without good cause. You can make Revoke future effective. If you know that a user is going to need access for a specific number of months, you may set the revoke date for the end of the last month the user needs access. This ensures that the user is revoked in a timely manner. If the user needs extended access, it is easy to change the revoke date to another. Revoke a user by putting a **current or future** date in the field. You must use the full year date (2014). If the user is Revoked, today's date shows in this field. Clearing the date resumes the user. Using Option 2 and entering the revoke and terminated dates is the preferred way to Revoke a user.

Revoked: Enter the current or future date for revocation in this field. This field will always show today's date, meaning the user is currently revoked.

Terminated: Enter the date that an APD employee left APD employment. **This date is for narrative purposes only and does not result in any other action.** This date will always remain the same as what was entered.

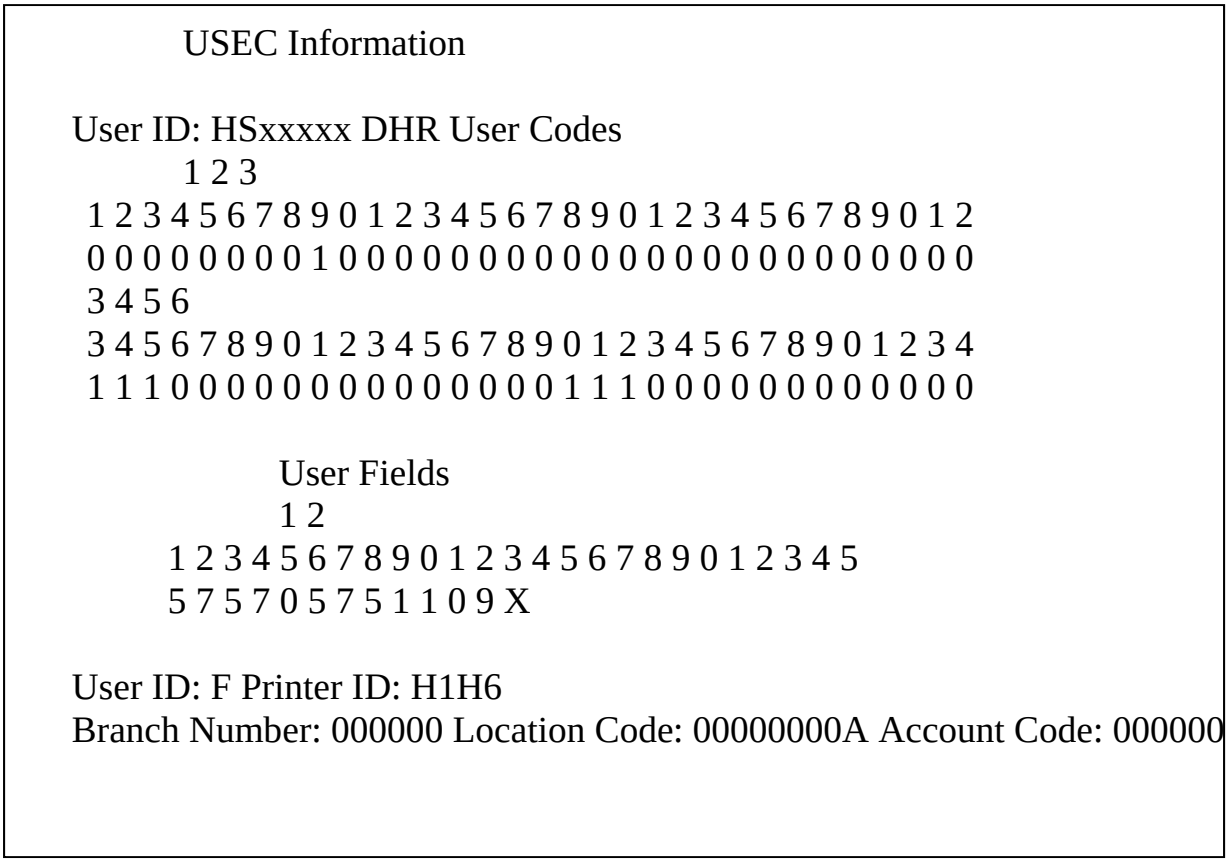
Comments: Enter the reason you revoke a user so that others know how to handle subsequent actions, and end your narrative with your initials. This is a free form comment section and can be used in any way you want in addition to the mandatory explanation of revoke.

It is required that you narrate on any user that you revoke. This is the only way we can prevent other sub-administrators from unknowingly restoring users in error.

Building the USEC Profile Data - (USEC File)

The USEC file is part of the RACF User Profile. It is built either by using the modeling method or by the RACF Administrative Screens displayed below. Branch sub-administrators cannot use the USEC screen so they must use the Modeling process. The Chief Data Steward can use the following screen. All users must have their profile completed with USEC codes or they will have incomplete access. Branch sub-administrators must call the Chief Data Steward if their staff cannot access or update transactions, or to have any of the table data below changed on a RACF User Profile. The exception is the Printer ID, Branch ID and Account Code.

This screen is only available to the Chief Data Steward.



F1=Help F3=Cancel Enter=Process

RACF/CICS System Change Timing

When any data in the RACF user profile is created, added or changed, it takes a specified period of time for the change to become active. The user must log off the terminal, wait the required time and then sign back on before the change will be available.

- Resuming or changing a password is immediate, after logging off and signing back on.
- Adding a new user takes effect immediately.
- USEC information takes 30 minutes of non-use.
- Immediate printer ID and branch ID changes can be made by the user through the use of the PSET utility program, if this has been authorized by local

management Original default values are reset overnight.

- Changes in User Group assignment take place immediately.
- CICS bits are updated overnight.

Suggestions

1. Do not create false Userids. The RACF data file must be kept free of data not directly related to a real user. We do not want any user to gain access to confidential information through false IDs that we “forget” about. If you create a Userid in error, please notify the Chief Data Steward.
2. You may have an infrequent occasion when, after entering a full screen of information and trying to update the record, you get a message “file not available.” This happens when an Analyst is using the file. DHS will try to store your screen until the file is available. You should then press **{ENTER}** to update your file. You can see if the update was completed by using the **Display User** screen.
3. Remember to use the comment lines on the user’s profile if important changes are made.