Option 4 Password Reset

The IPAC Agency Administrator is responsible for password maintenance on their user's accounts. New users are enrolled into the IPAC System using *Option 1 Create User* from the **Enrollment Main Menu**. After the User Roles Confirmation screen has been received, the user has been registered in the system and their system generated Login ID has been created. Then the user's initial password must be set using this menu option before the user can access the IPAC system. This menu option is also used by the IPAC Agency Administrator to perform password resets. Password resets may be needed in situations where the user has forgotten his password or the user has been locked out of the system after three unsuccessful attempts to enter his password.

All User Passwords stored for the IPAC system applications are first encrypted. When a new password is entered by a user, the application will audit the requested password to ensure that it meets security policy format requirements. If the password is cleared by the internal security audit, it is encrypted before it is stored to any permanent media.

All password exchanges are one way, from the user (or administrator) input into the IPAC system. There is no facility for the redisplay of a password by the system. The password collection function allows the appropriate user (or administrator) to enter a new password and then to retype the password for verification. On entry, the password characters are not displayed as typed. Rather, an asterisk (*) is displayed in the appropriate screen field for each character typed.

Since the passwords are encrypted, if a user password is forgotten, an Administrator cannot simply view the password and remind the user of its value. The Administrator must set the user's password to a temporary value that the user must then change on his next login.
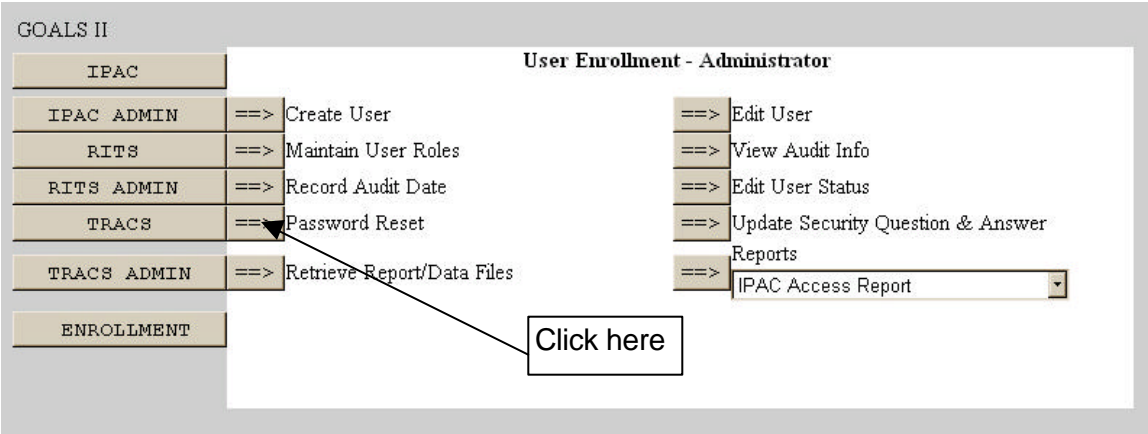

Figure 1.17   Enrollment Main Menu

To access the Password Reset function, select the "Password Reset" button from the **Enrollment Main Menu** as shown in Figure 1.17. The screen in Figure 1.18, **Find User** will display.

Retrieve the User's Record

This screen is used to retrieve the record of a user who is currently in the IPAC database. The process for retrieving a user's record is explained in detail in the *Introduction* to this manual.

Figure 1.18   Find User

When you have retrieved the user's record, the screen shown in Figure 1.19, **Reset Password**, will display.

Reset Password

Figure 1.19   Reset Password

Since most password reset requests will come to the administrator by telephone or email, the Administrator's **Reset Password** screen displays the Security Question and Security Answer previously entered for the Login ID. These are tools to verify the identity of the user for whom you are resetting a password. If a Security Question and Answer have been entered, the Administrator should ask the Security Question of the user and verify that the user's answer matches the Security Answer shown on the screen.

Once this verification has been made, the Administrator can enter a new password for the user and tell the user what his new password is. Administrator assigned passwords are only valid for one use. The user will be allowed to use the password to login to the system, but he must then immediately change his password to a new character string which meets the system requirements for a valid password.

Password Guidelines

The following is a list of guidelines to follow when setting up passwords:

- The maximum number of characters that can be repeated sequentially in a user password is 2. "123#depXX" could be set as a password because it does not exceed two "X" repeated characters. A password of "123#deXXX" could not be set as a password because three "X" characters exceed the limit of 2 repeated characters.

- The minimum number of letters of the alphabet that must be used for a password is 2.

- The minimum number of non-alphabetic characters (numbers, signs, special characters, etc.) that must be used for a password is 3.

- The minimum number of different characters that must be used for a password to be valid is 5. If the password specified is "0AbcbcA0", the password would not be valid because it only contained four different characters (0, A, b, c).

- The minimum length for a password is 8 characters.

- IPAC system passwords are case sensitive.

Type the new password for the user in the data entry box labeled Password. On entry, the password characters are not displayed as typed. Rather, an asterisk (*) is displayed in the appropriate screen field for each character typed. Verify the password you have just entered by typing the same password in the Re enter Password data entry box.

The two character strings that you just typed will be compared to ensure that they are identical. If they match exactly, the password will be audited by IPAC system to verity

that it meets security format requirements. If both of these criteria are met, the screen shown in Figure 1.20, **Password Reset Confirmation**, will display.

Password Reset Confirmation

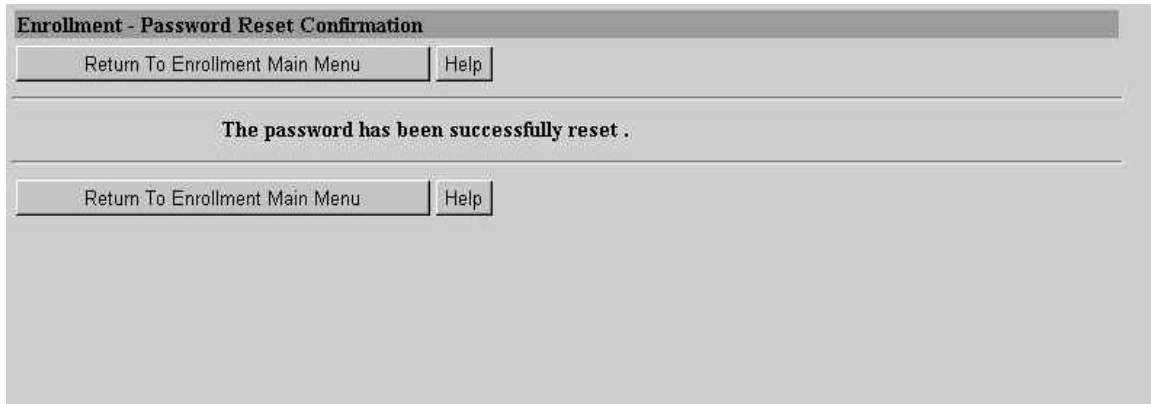| Enrollment - Password Reset Confirmation |
| Return To Enrollment Main Menu   Help |
| The password has been successfully reset . |
| Return To Enrollment Main Menu   Help |

Figure 1.20   Password Reset Confirmation

This screen confirms that the password has been successfully reset and you can inform the user of his new, temporary password. Select "Return to Enrollment Main Menu" for more menu options.

After the Password Reset Confirmation screen has been received, the user's initial password has been established. Then the user must be informed of his Login ID and Password so that he can access the IPAC System. The IPAC Letter Report will generate a separate User ID and Password letter for each user. See *Option 10 Reports* from the **Enrollment Main Menu** for instructions on how to generate the Login ID and Password letters for each user that you have registered.