.02 One-e-App User Account Authorization

Complete the following to authorize users to access the One-e-App system:

- Access the One-e-App web site.
- The One-e-App USER LOG IN screen displays. Complete the following:

  Key adduser in the USERNAME field, using all lower case characters.

  Key password in the PASSWORD field, using all lower case characters.

  Click on NEXT, or press ENTER.
- The USER PROFILE screen displays. Complete the following:

  Key the account information in the appropriate fields. Key the user's d0 log in as the User ID.

  Click on NEXT, or press ENTER, to submit the request for authorization. A message displays when the submission is successful.
- Complete a J-125 form for the user, and forward to FAA Data Security. Include the following on the J-125:

  User ID (d0 log in)

  One-e-App User Profile

  User's e-mail address

  Both of the following:

  - "HEALTH-E-ARIZONA"
  - “TOPAZ USER"

  NOTE TOPAZ is software that enables the viewing and printing of electronic signatures.

When both the J-125 and the One-e-App User Account request is received, FAA Data Security completes the following:

- Identifies and selects the new user in One-e-App.
- Assigns the User Profile and location.

- Authorizes the One-e-App User Account.
- Contacts the user by e-mail informing the user the account has been authorized and is active.

  The e-mail also informs the user to log in to the new account on the One-e-App USER LOG IN screen for the first time, as follows:

  - Key the user's d0 log in in the USER ID field.
  - Key password in the PASSWORD field, using all lower case characters.

When a user logs in for the first time, One-e-App prompts the user to change the log in password from password to a new password. Key the new password following the formatting requirements in Passwords to Secured Systems. Key the new password again to confirm.

WARNING

Do NOT use another staff's User ID and password to access the One-e-App system. Information returned through One-e-App is secured, and is confidential. Misuse of the authorized access to One-e-App is a security violation.