

PASS User File Maintenance

Standard Operating Procedures:

Process Steps

- UF600 – Adding a New User after Go Live

UF600 – Adding a New User

Overview

Purpose:

To add a new user after an agency has gone live.

Performed By:

User's Supervisor/Manager

PASS Training Coordinator

Agency Security Officer

SOAR District Security Manager

Tools Used:

Procurement Automated Support System (PASS)

SOAR ACCESS

REQUEST/MODIFICATION/TERMINATION FORM

Technology Used:

Internet browser (e.g., Microsoft Explorer®)

Procedure Steps



Note: Any user (from the agency) who has access to PASS can fill out the eForm for the new user, not just the user's supervisor. The supervisor will still have to approve the eForm, however.

1. Identify the need to add a new user to PASS after the agency has gone live.
2. User's Supervisor adds the new user using the PASS User Maintenance Request eForm.



Reference: Refer to UF100 – Enter a New user or Job Aid: How to Enter a New User in PASS for more details on how to use the User Maintenance Request eForm.

UF600 – Adding a New User– *continued*

3. Enter information in the “Login” field for the User Name to be used when accessing PASS.



Note: There are several options for the Login field – Start with Option 1 and if it is not available, use the other Options.

Option 1: Enter the new user's Windows User Name (the one currently used to login to their computer). PASS will alert you if that Login is already used in the system.

Option 2: Enter the user's last name and first initial with no spaces and lower case.

Option 3: Use a logical combination of the two. For example, if a user's name is “Mary Poppins”, the first choice for the User Name should be her Windows login. If that's already taken, then “poppinsm” should be tried. If that is also taken, use a combination of the two (always lower case), such as “marypoppins” or “maryp”.

4. Add roles and associated permissions (if necessary).
5. Submit User Maintenance Request eForm once all the fields are complete.
6. User Maintenance Request is routed to the Agency HR Manager (for informational purposes).
7. User Maintenance Request is routed to User's Supervisor for approval.



Note: If any of the Approvers in the flow deny the request, the eForm is routed back to the submitter of the eForm. The request can be re-submitted and/or there may be a need for discussion amongst the approvers.

8. User Maintenance Request is routed to PASS Training Coordinator for approval.
9. PASS Training Coordinator schedules new user for training.
10. Once training is complete, PASS Training Coordinator approves the eForm.
11. User Maintenance Request is routed to the Agency Security Officer for approval.

UF600 – Adding a New User– *continued*

12. Agency Security Officer then checks the Login that the supervisor selected during step 3 to ensure that the name is appropriate (i.e., the Login is some logical combination of the user's name).
 - If Login is correct, continue with Step 14.
 - If Login is incorrect, continue with Step 13.
13. Agency Security Officer denies the request and comments that the supervisor should select another name.
14. Agency Security Officer carefully reviews and verifies the PASS roles and permissions information on eForm to ensure proper separation of duties are being maintained:
 - If PASS role/permission information is correct, continue with Step 16.
 - If PASS role/permission information is incorrect, continue with Step 15.
15. Agency Security Officer denies request and adds a comment regarding the changes that need to be made on the role/permission information.
16. Agency Security Officer obtains CICS logon from OCTO's Data Center by sending the user's name and last 4 digits of their SSN to infosec@dc.gov.

UF600 – Adding a New User– *continued*

17. Agency Security Officer sends an email to the user's supervisor to have the SOAR ACCESS REQUEST/MODIFICATION/TERMINATION FORM (SR 71) completed and signed with the appropriate authorizing signatures.



Note: The Agency Security Officer can provide the SOAR Access form to the Supervisor by going to the CFO intranet website: <http://cfo.in.dc.gov>.

Click on OFOS SOAR Training
Click on Obtaining a SOAR Logon ID
Select SOAR Access/Request/Modification/Termination Form.

18. Once received from the new user's supervisor, Agency Security Officer faxes the SOAR ACCESS REQUEST/MODIFICATION/TERMINATION FORM to the SOAR District Security Manager to have the proper SOAR permissions established for the CICS ID.
19. Agency Security Officer edits the User Maintenance eForm and adds the CICS ID to the COMMENTS section of the eForm.
20. Agency Security Officer saves comments. Clicks on View Request to review the remaining information on request.
21. Agency Security Officer approves request. The request is routed to SOAR District Security Manager.
22. SOAR District Security Manager checks the Login that the supervisor selected during step 3 to ensure that the name is appropriate (i.e., the Login is some logical combination of the user's name).
 - If Login is correct, continue with Step 23.
 - If Login is incorrect, the SOAR District Security Manager selects an appropriate Login.

UF600 – Adding a New User– *continued*

23. SOAR District Security Manager carefully reviews and verifies the PASS roles and permissions information on eForm to ensure proper separation of duties are being maintained:
 - If PASS role/permission information is correct, continue with Step 25.
 - If PASS role/permission information is incorrect, continue with Step 24.
24. SOAR District Security Manager denies request and adds a comment regarding the changes that need to be made on the role/permission information.
25. SOAR District Security Manager establishes the proper security profile in SOAR for the CICS ID found in the eForm comments that were entered by the Agency Security Officer.
26. SOAR District Security Manager edits the User Maintenance request eForm and updates the SOAR Login and BANK ID fields.



Note: The SOAR District Security Manager is the only individual who can enter SOAR ID information.

27. SOAR District Security Manager approves the request.
28. Now the User Maintenance Request eForm is complete and fully approved. PASS automatically emails the new User a randomly generated password and informs the user to check with his supervisor for his login (the name entered during step 3).
29. Exit procedure.