Integrated Host Warehouse (IHW)
Version 1.3.1

User Guide
For
General Argonne Users

Prepared by:
Argonne National Laboratory
Computer and Information Systems Division
January 2, 2008

Table of Contents

Table of Figures

1. Introduction

Welcome to the Integrated Host Warehouse (IHW). This application will maintain data related to all computer hosts at Argonne National Laboratory. Computing services and tools will use this warehouse as the authoritative source of information related to any host at the laboratory. This application is accessible only from inside the Argonne network through the web at https://webapps.inside.anl.gov/ihw or https://inside.anl.gov/ihw.

Comments and/or suggestions on the web site or the application functionality can be sent to ihw_admin@anl.gov.

This User Guide is intended to help familiarize general Argonne users with the design and process of requesting authorization to use the Integrated Host Warehouse (IHW) system.

Welcome to IHW!

2. ISAAC Authorization

Users are authorized to do tasks in IHW through roles in the IHW service of ISAAC (https://portalapp8.anl.gov/isaac). The users role is equivalent to IT Admins and is public-enrollment-request-enabled. This means any Argonne user may request enrollment in this role. An approval process will be followed to grant or deny the request.

Roles are hierarchical, meaning that any task authorized at a lower role is also authorized by default to all higher roles. For example, IT Admins (users) are authorized to edit hosts, thus CSPR and CSPO roles also are authorized to be able to edit hosts. Furthermore, CSPRs can create organizations under the division level, thus CSPO can also create organizations under the division level, but IT Admins, as a lower role, can not. If a user has a security level of CSPR or CSPO, that user also has authorization to be an IT Admin.

Once a user is added to a role in ISAAC, he/she can be used in that capacity and lower level roles in IHW as many times as needed without requiring to be added to ISAAC again. The highest role for any one user is listed on the User Detail page for that user (see IT Admin guide). If the highest role is “no_privileges”, the processes explained in the following sections show how to request a user to be authorized for a role.

2.1 IT Admin Role

The users (IT Admin) role is authorized to manage host information within the organization for which they are given access. It is possible to be an authorized IT Admin, receive training, and be on the mailing list without being assigned to any organization.

The process of managing users in the IT Admin role falls into three event-driven activities; adding a new member, reviewing membership, and removing a member, which are explained in the following sections. A flow chart of the authorization process is in figure 7.

2.1.1 Authorize an IT Admin User

If a new IT Admin is assigned, a request for authorization can be made by any Argonne user, including the new user. The CSPO authorizes the user. If the user is already in the users (IT Admin), CSPR or CSPO role of ISAAC, he/she is already authorized and do not need to be added to any other ISAAC group (See Review IT Admin Users section 2.1.3 for instructions on how to verify a user is in a role).

Any user may request addition to the users (IT Admin) role of the IHW service of ISAAC by following these steps.

1. Login in to https://portalapp8.anl.gov/isaac/ (contact the Help Desk at help@anl.gov or 2-9999 option 2 if unavailable)
2. Go to the Enrollment By Service tab (figure 1)

Figure 1: Enrollment By Service Tab

3. Choose the "IHW" service and "users" role under Select a Service and Role (figure 2). If you do not have these options available, see an IHW Project Team member at ihw_admin@anl.gov to be granted access.

Figure 2: Select a Service and Role

4. Use the Query People section (figure 3) to find new user to add.

Figure 3: Query People

5. Click the Add button (figure 4) next to the user to be added to group.

Figure 4: Add User

Once an IT Admin has requested authorization, the CSPO will review the user status and grant or deny authorization. An email will be sent to the user to notify him/her of their authorization status.

By following this process, ISAAC will check if the user is a foreign national and

send a notification to the added user and to all users in the CSPO role to notify of the user addition and foreign national status (not yet implemented). Furthermore, on a daily basis, another process reads the users in the users role and adds them to the itadmins@anl.gov mailing list. Finally, ISAAC will check the IT Admin question in that users' Job Hazard Questionnaire (JHQ) to ensure the user receives the proper training (not yet implemented).

Once an IT Admin is authorized, he/she can be granted access in IHW to the appropriate organization by their CSPR.

2.1.2 Remove a IT Admin User

If a user in the "users" role is terminated from the lab, ISAAC will automatically remove that user from the "users" role and send a notification to all users in the CSPO role to inform of the termination. Any user from the CSPO or CSPR role must then go to IHW and follow instructions in the CSPR User Guide to remove access from IHW.

If a user in the "users" (IT Admin) role transfers to another division, ISAAC will notify all users in the CSPO role of the transfer. One of the users must then follow instructions in the CSPR User Guide to remove access in IHW and follow the steps below to remove authorization for that user.

1. Login in to https://portalapp8.anl.gov/isaac/
2. Go to the Enrollment By Service tab (figure 1)
3. Choose the IHW service and users role under Select a Service and Role (figure 2).
4. Find the user to be removed in the Edit Enrollment section and change status to Inactive (figure 5).

Figure 5: Remove User from users Role

Once a IT Admin user is removed from the ISAAC users role the next daily run will remove them from the itadmins mailing list and uncheck the IT Admin question on that users' JHQ (not yet implemented). Note: The IT Admin question on the JHQ is fully controlled by the ISAAC users role; any changes made to the JHQ outside of ISAAC will be reverted by ISAAC (not yet implemented).

2.1.3 Review IT Admin Users

On an annual basis in October, ISAAC is set to notify all users in the CSPO role to review membership in the "users" (IT Admin) role. Any user notified may review and record verification with the following steps, although best practice is for CSPRs to review and send changes to CSPO for CSPO to do final verification.

1. Login in to https://portalapp8.anl.gov/isaac/
2. Go to the Enrollment By Service tab (figure 1)
3. Choose the IHW service and users role under Select a Service and Role (figure 2).
4. Verify users in role are the ones that are authorized.
5. If there are any unauthorized users, see section 2.1.2 to remove.
6. If there are any missing users, see section 2.1.1 to add.
7. Once list is valid, click the Record Enrollment Verification button (figure 6) to stop further email notification until next review cycle.

Figure 6: Record Enrollment Verification

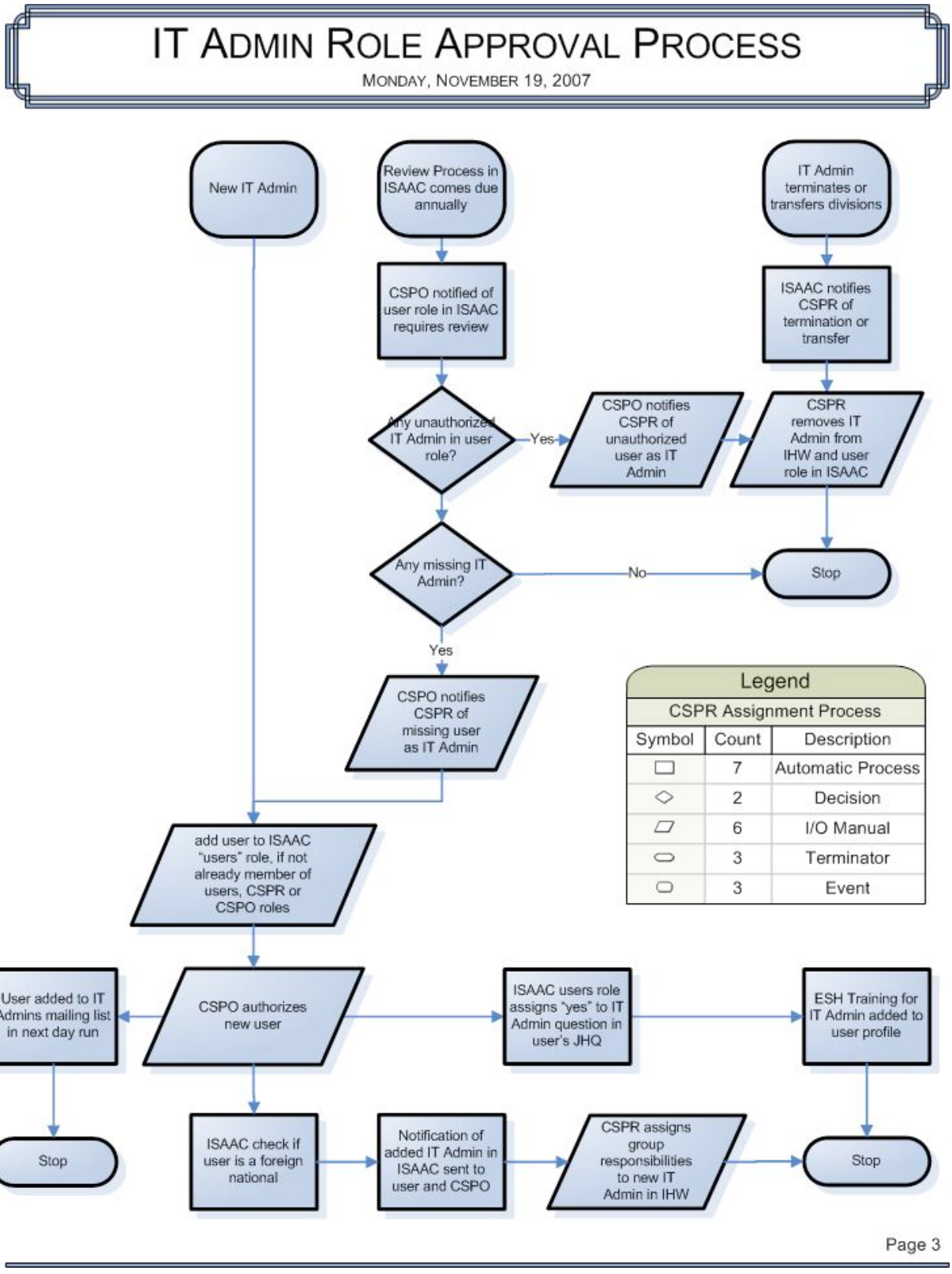

Figure 7: IT Admin Authorization Process Flow Chart