SUBMITTER PROCESS GUIDE

As an approved Submitter for the Kansas Eligibility Enforcement System (KEES), you have been assigned the responsibility of submitting New User requests and Current User Change Requests for your assigned group. In addition, you will also be responsible for obtaining, verifying, and forwarding required documentation to the ksc@kees.ks.gov mailbox prior to submitting a request. This document was created in order to assist you in completing the process of submitting KEES requests for NEW or CURRENT staff.

The KEES Repository

The KEES Repository contains detailed instructions regarding the OIM (Oracle Identity Manager) and how it is used to create New User requests. The necessary forms and documentation requirements for New User access may also be found in the Repository, along with the Submitter Training Document.

Save the KEES Repository link and review the following repository documents under KEES Security Access.

1. KEES Submitter Training Document: This document will walk you through the OIM process of requesting KEES access for a New User.
   The New User page has changed slightly from the version in the manual, but the process itself has not changed.

2. KEES Access Change Request Form: If you are requesting access for a User who is already known to the KEES system, you will need to fill out a KEES Access Change Request to reinstate access or make changes in their access, name, location, supervisor, etc.
3. KEES End-User Security Agreement Form: This form must be completed in its entirety and signed by both the User and Supervisor.

4. KEES Access Instructions: The KEES Access Instructions document details the required documentation for access to KEES.
   Before you enter a request in OIM, make sure the proper documents are sent to ksc@kees.ks.gov. If the documents are not received, or are incomplete, the request are returned to the Submitter.
   NOTE: If your agency's system does not provide Certificates after the training sessions, or users have trouble obtaining acceptable proof of training documents, suggest they use their Windows Snipping Tool to create a .jpg clip of their Transcript page. The Transcript includes all completed courses. Your local IT staff can help with that process if necessary.

Kansas
Eligibility Enforcement System (KEES)

I. New User – OIM Request

Only employees who have never had access to KEES Production are considered NEW USERS.

Staffs are identified in KEES first by their email addresses, and second by name. If an employee had KEES access in the past, left employment, transferred to another department, or has had their access Inactivated or Disabled, they are still considered a current user because their email address is already known to KEES. No one is ever removed from the system. They are just assigned a different status. Therefore, when you look up a potential new user in KEES and find that are already known to KEES (maybe from a previous email address), their account may display as Active or Inactive. In either case, you must not use OIM to create a New User. It will be necessary to use the KEES Change Request form to reinstate access or make any account changes. Remember to always check for previous access.

New User Requests:

STEP 1: Submit required Security Agreement and required training documentation for New User.

STEP 2: Create New User request in OIM.

STEP 3: Once your request has been completed in OIM, contact your assigned Approver and notify them that there is a TASK in OIM awaiting their approval.

NOTE: if all the required documentation for a New User has not been received prior to the submission of a New User Request in OIM, the Request (Task) will be returned to the Submitter. Once documentation is received, the Submitter can re-Submit the Task to the Approver. (See Heading III below - Responding to Requests for Information Tasks) or Page 12 of the KEES Submitter Training Document located in the KEES Repository.)

II. Current User – KEES Change Request

A Current User is defined as anyone who has, or has ever had, access to KEES Production. No User is ever deleted from the KEES Production system. The key identifier is the email address. Be sure to check the current user name and any previous names, against any possible 'old' email addresses under different names in KEES before you create a New User in OIM.

A. REINSTATE DISABLED USER IN OIM (In KEES, the status will be "Inactive.")

- Requires a KEES Change Request form. (Include in the Comments field that you would like to reinstate user.) NAME: INCLUDE MIDDLE INITIAL
- Requires a new KEES Security Agreement. (Send all 3 pages.)
- Requires an up-to-date Security Awareness Training document or copy of the User's Transcript (training date must be within the current year as the request).

B. NAME or EMAIL ADDRESS CHANGE

- Requires a KEES Change Request form.
- Requires a newly-signed Security Agreement that includes the new legal name. (Send all 3 pages.)
- Use the current (new) name as the User Name on the KEES Change Request form.
    - **NAME: INCLUDE MIDDLE INITIAL**
- Include a note in the **Comments** section that identifies the previous name.

- Verify the email address and all other data on the form.
- Include the User's KEES ID in the ID field when possible. This allows further verification of user.

C. REMOVE KEES ACCESS (left the agency or no longer needs KEES access)

- Requires a completed KEES Change Request form. Mark the 'Remove All Access' box on page 2.NAME: INCLUDE MIDDLE INITIAL

D. TRANSFERS

Losing Office –

- The losing office will fill out the Change Request form and check the box at the top of the page to "Remove all KEES Access." User status in KEES will be changed to Inactive, and OIM will show the user as Disabled.
- The Supervisor will end-date the current Worker ID.

Gaining Office –

- Send a newly-signed Security Agreement and a copy of the employee's Learning
- Center transcript to verify security awareness training is up-to-date.
- Submit a KEES Change Request to reinstate the staff member under the new office.
- In the Comment Section, include the reason for reinstatement – "User transferred from <value> to <value> ."
- Supervisor of new location will assign a new Worker ID if necessary.

E. LOCAL CHANGES

Supervisor (Same Department)

- If nothing changes other than the user's Supervisor, the new Supervisor may send an email to the ksc@kees.ks.gov mailbox with their name and email address and the full name and email address of the employee.
- Supervisors are responsible for changing the Worker ID when necessary.

Position (Results in Access Change)

- Fill out the KEES Change Request and include any information that has changed.
  - **NAME: INCLUDE MIDDLE INITIAL**
- Add a note in the Comments section to summarize the request.
- Supervisor will make any Worker ID changes when necessary.

Security Group/Access Add/Change

- Fill out the KEES Change Request and include any information that has changed.
  - **NAME: INCLUDE MIDDLE INITIAL**
- Add a note in the Comments section to summarize the request.
- Supervisor will make any Worker ID changes when necessary.

Department/Unit

- Fill out the KEES Change Request and include any information that has changed.
  - **NAME: INCLUDE MIDDLE INITIAL**
- Add a note in the Comments section to summarize the request.
- Supervisor will make any Worker ID changes when necessary.

III. Responding to "Request for Information" Tasks

The following process should be followed when an Approver or the Security Administrator returns a Submitter's Request (Task) for more information. Examples of reasons for a returned Task may include:

- Documentation has not been received
- Documentation is unacceptable or illegible
- The Group Access code is questionable
- The name and email address do not match and an explanation is not included in the Comments section.

When a Submitter's request is returned for more information, it will be returned as a TASK. Follow the instructions below for a Task that is waiting for more information:

STEP 1: Sign on to OIM and click the **Task** tab.
STEP 2: Click the **Approvals** tab and a list of any returned **Tasks** display.
STEP 3: Click the **Task ID** to view the **Task Details**.
STEP 4: Under **Additional Request Information**, a note from the sender displays telling you exactly what is missing or questionable.
STEP 5: Once you have sent in the missing documentation or otherwise complied with the request, select the **Additional Request Information** box again.
STEP 6: Click inside the box below the requested information, and it expands to allow you to enter a response.
STEP 7: Enter your response and click **Submit to Approver** at the top of this tab.
STEP 8: A pop-up box tells you if the Task has been submitted successfully.

NOTE: From the Approval Tab, you can view the Details of the request, view any previous Request Comments, or pull up the History for this Task.

FAQ

Q: How can we tell in KEES if a person no longer has access or never had access?

A: Anyone who has EVER had access to KEES Production will show up on the Staff Search page.

Look up every new, potential KEES user to make sure they do not have a previous name or email address associated with KEES. If their name appears, and the email address is (or was) a valid email address for the person, they have had or currently have access, and you will need to submit a KEES Change Request to reinstate the user and make necessary changes.

Q: If a User calls the KEES Helpdesk and is told their access has been Disabled, what does that mean and what must be done to regain access.

A: The KEES Helpdesk uses the OIM system to verify access when users call for password resets, etc. When a Helpdesk technician says access has been "Disabled," it means the user had previous access but is no longer active. It will display as "Inactive" in KEES, but OIM will reference the user as "Disabled." A Change Request to "Enable Previous Access" and a newly- signed KEES Security Agreement is required for reinstatement. In addition, a new Security Awareness training documentation may be required if the one on file is not up-to-date (completed within the same year as the Change Request).

Q: When you first create a New User request in OIM, is it necessary to include a Worker ID, or can a supervisor assign one once the worker has access?

A: The Worker ID can only be assigned AFTER access has been created for the user. If it is not included on the New User Request in OIM, the Supervisor must assign it for the staff member after they receive access but before they actually do any work in KEES. The Worker ID is connected to several different functions and those functions will not work without a Worker ID. (Example: Journaling will not work without a Worker ID.)

It is not REQUIRED that supervisors include the Worker ID in the OIM New User request. However, doing so eliminates the need for supervisors to enter one in KEES themselves, and this may sometimes prevent unnecessary issues.

Example: The request is submitted w/o a Worker ID but the Supervisor does not know when the User has received their access. The user logs on, a particular function does not work as expected, the User calls the Helpdesk, and a ticket is created. A simple Worker ID assignment in the OIM New User request would have prevented the issue.

Q: Who should send in documentation?

A: Although it does not matter who sends in Security Agreements and Training Documentation, it is the responsibility of the Submitter to make sure that documentation has been sent to the ksc@kees.ks.gov mailbox prior to creating a New User request. If proper documentation is not on file when the request is received by the Security Administrator, the Request Task will be returned to the Submitter for lack of documentation. When sending in a Change Request, the documentation should be attached to the same email address that contains the Request.