

# Kuali@USC Quick Reference Guide: Kuali User Access Request Document

In the USC Kuali system, transactions and database changes are submitted in electronic documents called “eDocs.” This guide presents instructions for creating and submitting the **User Access Request Document**, which is a Kuali Enterprise Workflow (KEW) eDoc that is used to request that specific access rights within Kuali and its related systems be added, changed, or deleted for a given user.

This guide offers instructions for the User Access Request Document eDoc in Kuali, but does not cover introductory information, such as general descriptions of the Kuali on-screen interface or explanations of workflow routing. For that information, please see the separate document titled **Kuali Basics: Reference and Training Guide**, which can be accessed here: <[www.usc.edu/kuali/basicsguide](http://www.usc.edu/kuali/basicsguide)>

If you need assistance, please call ITS Customer Support at 213-740-5857 (UPC) or 323-422-1968 (HSC).

<b>CONTENTS:</b>	
General Information About the KEW User Access Request Document .....	2
Initiating a User Access Request Document .....	2
Adding Notes or Attachments .....	5
Importing Multiple Lines of Data .....	6
Submitting Your User Access Request eDoc .....	7
Saving an eDoc Before You Are Ready to Submit It .....	8
Resubmitting an eDoc Returned for Correction .....	8
Checking the Status of a Submitted eDoc .....	8
Creating a User Access Request Document by Copying an Existing One .....	9
Logging Out of the Kuali System .....	10
<b>Kuali Financial System (KFS) Modules</b>	
Cashiering .....	11
Procurement Card Reallocation .....	12
Purchasing - Accounts Payable (USC eMarket) .....	13
Payroll Expense Transfer & Effort Certification .....	17
eStatement .....	18
Journal Vouchers (JVs) .....	20
Disbursement Vouchers (DV/DVQE) .....	20
Internal Billing .....	24
General Budget Change .....	24
Capital Assets Management (CAMS) .....	24
SPA Budget Reallocation .....	26
<b>Kuali Enterprise Workflow (KEW) Modules</b>	
General Purpose Workflow .....	26
Financial Aid Account (FAA) .....	27
Chart of Accounts (COA) .....	29
Course Scheduling .....	29
<b>Account Level, Organization Code Level, Payroll Reporting, and BI Planning &amp; Projections Access</b>	
Add Account Access (Inquiries, Payroll Expense Transfer, and Reports) .....	31
Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports) .....	33
Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports) .....	35
Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports) .....	37
Payroll Business Intelligence Reporting Access .....	38
BI Planning and Projections (P&P) .....	40
Other Requests .....	40
INDEX .....	41

## General Information About the KEW User Access Request Document

The KEW User Access Request Document is a Kualo eDoc that is utilized to request that specific access privileges within Kualo and its related systems be added, changed, or deleted for a given user.

Although users requesting access privilege changes can initiate this eDoc for themselves, it is anticipated that the User Access Request eDoc will most often be completed and submitted for those users by someone designated as a User Access Coordinator for his or her department, school, or business unit.

**NOTE:** This document can only be used to request user access to Kualo and its linked systems, such as USC eMarket and the Business Intelligence Portal for KFS. It does not apply to older existing financial systems, such as WebBA, Viador Data Warehouse, and FDL (Financial Download system).

## Initiating a User Access Request Document

Use this procedure to create a new User Access Request eDoc. For instructions on copying an existing User Access Request eDoc to create a new one, see *Creating a User Access Request Document by Copying an Existing One* on page 9.

1. Click the Kualo login link on either the [USC Employee Gateway](#) or [Kualo@USC website](#).  
The **USCnet Login** page will be displayed.
2. Log in, using your USC NetID user name and password. The **Financial Main Menu** page of the Kualo screen will be displayed.

If you do not know your NetID or password, please call ITS Customer Support at 213-740-5857 (UPC) or 323-422-1968 (HSC).

**TIP:** It is strongly recommended that you create a browser bookmark to the Financial Main Menu page for easy access to the Kualo system. When you later use that bookmark, you will be directed first to the "USCnet Login" page and then to the Financial Main Menu page once you have logged in.

3. Select the **Workflow Main Menu** tab near the top of the Kualo screen. The Workflow Main Menu page will be displayed.
4. On the Workflow Main Menu page, click the **User Access Request Document** link, which is located in the upper left-hand portion of the screen.

The screen will change to display the form for the User Access Request Document. Fields marked with an asterisk (\*) are required, and must be completed in order to submit the eDoc. In the upper right-hand area of the screen, the fields for document number, status, Initiator, and the creation date will be populated by the system.

5. In the *Description* field in the uppermost folder tab, labeled **Document Overview**, type a brief description (40 characters max.) to identify the user access request you are submitting. (Below the *Description* field, the *Organization Document Number* field is not in use at this time.)

When completing the *Description* field, you should include the name of the applicant for whom this access request is being submitted, the type of access change (addition, deletion, etc.), and the Kualo module to which the access change pertains, as space permits in this field. No changes will be made to existing access unless specifically requested.

Also, if the eDoc will contain requests for multiple access additions or deletions, or access requests for more than one Kualo module, please include the word "multiple" in the description you enter.

**NOTE:** The eDoc you are creating could appear in the results of a document search performed by any Kualo user. Therefore, do not include any sensitive information in the *Description* field because the contents of that field will be visible in the search results.

6. The *Explanation* text box is an optional field. If desired, use it to enter additional notes or a continuation of the information you have entered in the *Description* field.
7. Complete the folder tab labeled **Applicant Information**, as follows:
  - a. If you are initiating this eDoc to request user access changes for yourself, simply select the *Same as preparer* checkbox.
  - b. If you are initiating this eDoc to request user access changes for someone else, enter **either** the 10-digit USC Identification Number **or** the 7-digit Employee ID Number for that user in the appropriate field, and then press the TAB key or click on another field. The system will automatically populate most of the other fields with identification and contact information on file for the applicant, with the following exceptions:
    - The applicant's Middle Name is not required, but can be entered if desired.
    - **Department Organization Code** is a required field, but is not populated automatically, so you must enter the complete 10-digit number yourself. Note that this is not the applicant's Home Department Code; it is the Organization Code that identifies the account credited and debited for the transactions of the department with which the applicant is associated. You should be able to obtain the code from the applicant's SBO or supervisor.

The Organization Code, which was called a "Program Code" in the legacy WebBA system, is a 10-digit number that identifies an accounting center (e.g., a school or an administrative unit) and all of the departments within that center. Every account used for financial transactions belongs to an Organization Code so that it is possible to identify the center responsible for that account.

In the Kualii system, the Organization Code appears in the results displayed for either an **Account Lookup** or any of the General Ledger balance inquiries. It also appears on the Account Status Report (ASR) in both WebBA and the Business Intelligence GL reports for Kualii.

To find which Organization Code to use for your assigned department, choose one or more of the accounts that you use for transactions on a regular basis, and note the Organization Code associated with those accounts. You may have more than one, so pick the one that identifies your main accounting center.
8. The folder tab labeled **Preparer Information** is automatically populated by the Kualii system, using information on file for your user login ID.
9. When you are ready to proceed, click the  button.

The bottom portion of the on-screen eDoc form will expand to display several more folder tabs in addition to the ones shown previously. One of the added folder tabs, **View Applicant's Current Access**, will appear between the **Applicant Information** tab and the **Preparer Information** tab.
10. The **View Applicant's Current Access** tab contains a link that enables you to view the access rights already assigned to the applicant. When you click that link, the results of a **Person Lookup** for the applicant will be displayed in a new window or tab (depending on your browser settings). On that results page, click the  button on the **Membership** tab to view the applicant's current access information.

**NOTE:** If you need assistance in understanding the information shown on the **Membership** tab, please consult your department's User Access Coordinator or SBO.

11. On the **Module Selection** folder tab, select the appropriate check-box for each Kualii module to which you are requesting new or different user access privileges.

Although this eDoc is designed to accommodate access requests for more than one module, the applicant for whom you are submitting the request will probably need access to just one module in most instances. However, it is also common for a user to need access to multiple accounts.

When you select the check-box for a particular module, the corresponding folder tab in the lower portion of the eDoc form will open. You can see a pop-up description of each module by placing your cursor over its check-box.

**NOTE:** The check-box for *Pre-Encumbrance* is not currently active, but is reserved for future use.

Be sure to also select the *Add Account Access* or *Add Organization Code Access* check-box if you are requesting access rights to specific accounts for the applicant. Likewise, select the *Remove Account Access* or *Remove Organization Code* check-box if you are requesting the removal of access rights for specific accounts.

12. From this point, proceed to the sections of this guide that pertain to the specific types of user access changes that you are requesting. When you have completed the tabs associated with all the changes you are requesting, proceed to the **Submitting Your User Access Request eDoc** instructions on page 7 of this guide. If you need to attach any related files to your request, refer to the **Adding Notes or Attachments** instructions on page 5.

The following table presents an alphabetical list of the access-related tabs currently in use on the User Access Request eDoc with the page numbers on which you can find the instructions for each tab. You can click on a tab name or its page number to proceed directly to the relevant section of this guide.

**Access-Related Tabs on the User Access Request eDoc (listed alphabetically)**

- |  |   |
|--|---|
| • <b>Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 31]           | • <b>General Purpose Workflow</b> [page 26]   |
| • <b>Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 35] | • <b>Internal Billing</b> [page 24]   |
| • <b>BI Planning and Projections (P&amp;P)</b> [page 40]   | • <b>Journal Vouchers (JVs)</b> [page 20]   |
| • <b>Capital Assets Management</b> [page 24]   | • <b>Other Requests</b> [page 40]   |
| • <b>Cashiering</b> [page 11]  | • <b>Payroll Business Intelligence Reporting Access</b> [page 38]                                     |
| • <b>Chart of Accounts (COA)</b> [page 29]   | • <b>Payroll Expense Transfer &amp; Effort Certification</b> [page 17]                                |
| • <b>Course Scheduling</b> [page 29]   | • <b>Procurement Card Reallocation</b> [page 12]  |
| • <b>Disbursement Vouchers (DV/DVQE)</b> [page 20]   | • <b>Purchasing - Accounts Payable (USC eMarket)</b> [page 13]  |
| • <b>eStatement</b> [page 18]  | • <b>Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 33]           |
| • <b>Financial Aid Account (FAA)</b> [page 27]   | • <b>Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 37] |
| • <b>General Budget Change</b> [page 24]   | • <b>SPA Budget Reallocation</b> [page 26]  |

**IMPORTANT:** Several of the tabs on the User Access Request eDoc include an *Actions* column. When completing any of those tabs, remember that **you must click the  button** in the *Actions* column or the line of information you have entered will not be saved as part of the eDoc.

## Adding Notes or Attachments

If you need to add any general comments or attachments to the User Access Request eDoc, follow these instructions to complete the **Notes and Attachments** tab.

1. On the folder area labeled *Notes and Attachments*, click the **show** button to reveal the fields and controls used for adding comments and attaching related files.

2. Click the **Browse...** button next to the *Attached File* field and navigate to the location of the file on your computer that you want to attach to this eDoc. The full path of the file that you have selected will appear in the *Attached File* field, but it is not yet attached.

Notes and Attachments		Posted Timestamp	Author	* Note Text	Attached File	Actions
add:					<input type="text"/> <input type="button" value="Browse..."/>	<input type="button" value="add"/>

If you want to change your selection to a different file, click the small **CANCEL** button just below the *Attached File* field. When that field is empty again, click the **Browse...** button once more to locate the other file that you want to attach.

3. Before attaching the file that you have selected, you must type the name of the file or a brief descriptive comment in the text box labeled *Note Text*. (This is a required field.)
4. To attach the file that you have selected, click the **add** button located to the right of the *Attached File* field.

When you have finished entering all the requested information, proceed to the **Submitting Your User Access Request eDoc** instructions presented next in this guide.

## Importing Multiple Lines of Data

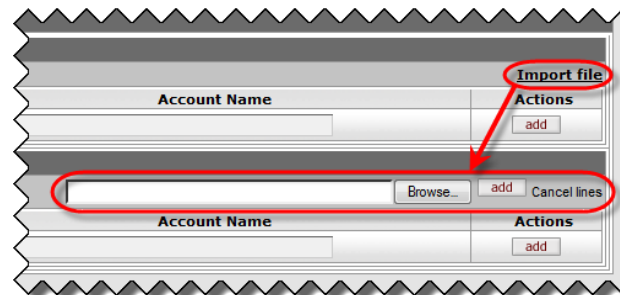
Several tabs on the User Access Request eDoc include an **Import file** link above the *Actions* column. This link enables you to import multiple lines of data at once for one particular field on the tab in question. In each such instance, the type of data that can be imported varies depending on the field to be populated, as noted in the following table:

<i>Tabs on the User Access Request eDoc</i>	<i>Field Data That Can Be Imported</i>
<b>Procurement Card</b>	Organization Codes (10 digits, OR a 5- or 7-digit mask)
<b>Purchasing - Accounts Payable</b>	Account Numbers (10 digits, OR a 4- or 6-digit mask), or Department Organization Codes (10 digits only)
<b>eStatement &gt; Business Office Reviewer: Add BOR Access / Delete BOR Access</b>	Organization Codes (10 digits, OR a 5- or 7-digit mask)
<b>Journal Vouchers: Add Access / Delete Access</b>	JV Numbers (3 digits only)
<b>Add Account Access</b>	Account Numbers (10 digits, OR a 4- or 6-digit mask)
<b>Remove Account Access</b>	Account Numbers (10 digits, OR a 4- or 6-digit mask)

To utilize this function, follow these steps:

1. Create an Excel worksheet file consisting only of a single column that contains all the data to be imported, with one entry per cell. If the type of data that you will be importing includes any “masks,” be sure to type them as unbroken strings of digits ending with an asterisk (\*).
2. Save the Excel file in the **.CSV** (comma-separated value) format. Be sure to note the location where you have saved the resulting **.CSV** file.
3. Click the **Import file** link on the tab to which you want to import the data from your **.CSV** file. The link will then be replaced by other controls, as shown in the following screen image:

If you want to cancel the import task, click the **Cancel lines** link. Otherwise, proceed to the next step.






4. Click the **Browse** button to open a dialog box that will enable you to navigate to the location of the **.CSV** import file you saved.
5. Select your import file and click the **Open** button.
6. When the name of the desired import file is displayed in the field next to the **Browse** button, click the **add** button. The data from your **.CSV** file will be imported onto individual lines in the destination tab.
7. After the line entries have been imported from your **.CSV** file, you can manually add other lines if desired, or make any changes that may be needed in the imported lines.


## Submitting Your User Access Request eDoc

When submitting the KEW User Access Request Document eDoc, you **must** complete the *Person Requests* section of the **Ad Hoc Recipients** tab as explained in this section to ensure that the eDoc is routed to the appropriate Senior Business Officer (SBO) for approval. This eDoc cannot be submitted and processed unless at least one ad hoc recipient has been specified. After it has received all ad hoc approvals, the eDoc will automatically be routed to the “SysAccess” group in the Office of the Comptroller for processing.


- In most instances, where you are submitting the eDoc for an applicant who is not an SBO, you will need to route the eDoc to the SBO of the applicant’s department or school.
- If you are submitting the eDoc for an applicant who **is** an SBO, it must be routed to him or her for the required approval.
- If you are submitting the eDoc to request access changes for yourself and you are an SBO, then you need to route the eDoc to yourself for approval.

Use the following procedure to complete the **Ad Hoc Recipients** tab:

1. Select the APPROVE option from the *Action Requested* drop-down list in the *Person Requests* section on the **Ad Hoc Recipients** tab.
2. In the *Person* field, enter the User ID of the person to whom you want to route the eDoc. If you need to search for the User ID of the intended recipient, click the lookup icon  next to the *Person* field. Use the fields provided on the **Person Lookup** page to enter search criteria. When the search results are displayed, click the *Return Value* link for the desired person, and the *Person* field on the eDoc page will be populated automatically.
3. Click the  button in the *Actions* column.
4. If all other sections of the eDoc have been completed and you are ready to submit your User Access Request Document, click the  button at the bottom of the eDoc screen. The Kualo system will validate your eDoc (i.e., check it for errors) and then refresh the page displayed in your browser.

When the refreshed eDoc page appears, scroll to the top of the screen in order to view the status of your eDoc submission. The status message will state “Document successfully submitted” if there were no errors found in your eDoc. If the status message indicates that there were errors in your eDoc, such as missing information, take note of the problem and make the necessary changes or additions to the information you entered. After correcting your eDoc, click the  button again, and then check the new status message to see if any further adjustments are needed.



If you later want to check on the status of an eDoc you have submitted, refer to the instructions presented in **Checking the Status of a Submitted eDoc** on page 8 of this guide.


If you want to perform additional User Access Request transactions, click the  button at the bottom of the screen, click Yes if you are asked to confirm your action, and then select the **User Access Request Document** link again from the Workflow Main Menu screen.

If you want to exit the Kualo system, see the **Logging Out of the Kualo System** instructions on page 10.


### Saving an eDoc Before You Are Ready to Submit It


There may be times when you cannot finish entering information for a User Access Request eDoc in one sitting, or you might need to postpone submitting it. On those occasions, you can save the eDoc without losing any of the information that you have entered.

When you click the  button at the bottom of the screen, all the information you have entered will be preserved so you can return to it later. The eDoc that you saved will wait in the Inbox of your Action List, which you can access by clicking the  button located in the upper left portion of the Main Menu screens.

When you are ready to complete an eDoc that you previously saved, open it from your Action List, finish entering all required information, and then click the  button at the bottom of the eDoc screen.


### Resubmitting an eDoc Returned for Correction

You may occasionally receive an email message from the Kualu system informing you that a User Access Request eDoc needs your attention. The email message will contain a link that you can click to access the eDoc in question. You can also open the eDoc from the Inbox of your Action List, which you can access by clicking the  button located in the upper left portion of the Main Menu screens.

Once you have opened the eDoc that requires changes, look at the **Notes and Attachments** tab to find out what information you will need to revise or add. After you have made the required changes or additions to the information you entered when you originally submitted the eDoc, click the  button at the bottom of the screen to resubmit the eDoc.

### Checking the Status of a Submitted eDoc

Use this procedure to learn the current status of a User Access Request eDoc after you have submitted it.

1. Log into the Kualu system, as described in *Initiating a User Access Request Document* on page 2 of this guide.
2. Near the top of the Kualu screen, click the  button.  
The **Document Lookup** page will be displayed.
3. Type your user name in the *Initiator* field.

**TIP:** If you are unsure of your user name, note that it is displayed after “Logged in User:” in the upper right-hand area of the Kualu window.

4. Use the date selector tools adjacent to the *Date Created From/To* fields to specify the date range during which you submitted the eDoc in question. You can also further refine your search by entering the document type abbreviation (*UAM* in this case) in the *Type* field.
5. Click the **Search** button.  
The search results, consisting of all the eDocs that you submitted during the specified time period, will be displayed in a table at the bottom of the screen.
6. In the search results table, identify the eDoc whose status you want to check, and click the document icon at the rightmost end of the same row, in the column labeled *Route Log*.  
The screen will change to display status information for the eDoc in question, so that you can see where it is in the approval process.



### Creating a User Access Request Document by Copying an Existing One

The Kualii system provides a way for authorized users to initiate a new eDoc based on a copy of one that already exists. This method of creating a new eDoc may be useful when an existing eDoc contains enough of the relevant data to be entered in the new eDoc that only a few minor changes or additions are needed.


Copying an existing eDoc will create a new eDoc of the same document type, with its own new Document ID number, but otherwise reproducing most of the same data entry details and settings contained in the original eDoc. Note, however, that any attachments in the original eDoc will not be copied to the new eDoc, and some details from the original eDoc may not appear in the new copy.

To create a new User Access Request eDoc by copying an existing one, use the following procedure:


1. Use the **Document Search** function in Kualii to find the existing User Access Request eDoc that you want to copy.
2. In the list of search results, click the hyperlinked Document ID number of the desired eDoc to open it.  
Your browser will then display the eDoc that you selected.
3. At the bottom of the displayed eDoc, click the **copy** action button.  
Your browser window will be refreshed to display a new User Access Request eDoc with a new Document ID number in the document header in the upper right-hand corner of the eDoc screen. The document header will also contain a *Copied From* field that identifies the Document ID number of the original eDoc from which the new one was copied. (Additionally, a note identifying the original eDoc will appear in the **Notes and Attachments** folder tab.)
4. Just below the document header fields in the upper right-hand corner of the eDoc screen, click the **expand all** button to expand all of the folder tabs in the eDoc form.

**NOTE:** All of the completed tabs from the original eDoc will be reproduced in the new eDoc, even if their corresponding check boxes on the **Module Selection** tab are not selected.

5. Carefully review all of the populated (i.e., not empty) tabs on the eDoc and remove any data in completed tabs that are not part of the new access request you are submitting.
6. Return to the top of the eDoc and click the **collapse all** button to close all of the expanded tabs.
7. Click the **show** buttons at the tops of the following tabs to open them:
  - **Document Overview**
  - **Applicant Information**
  - **View Applicant's Current Access**
  - **Preparer Information**
  - **Module Selection**
8. On the **Module Selection** folder tab, select the appropriate check-box for each Kualii module to which you want to request new or different access privileges for the applicant. If any of the check-boxes for other tabs are selected, be sure to clear (de-select) them.  
The folder tabs corresponding to the check-boxes you have selected will open in the eDoc form.
9. Complete the tabs pertaining to the specific access request you want to submit. Be sure to change or delete any data or settings reproduced from the original eDoc that are not relevant to the new access request you are submitting.

10. Ensure that the *Person Requests* section of the **Ad Hoc Recipients** tab is completed properly, as described in **Submitting Your User Access Request eDoc** on page 7.
11. When all relevant sections of the eDoc have been completed and you have deleted data from the original eDoc in all unrelated tabs, click the  button at the bottom of the eDoc screen.

### Logging Out of the Kualo System

There is no “Log Out” button or link in the Kualo system. To exit Kualo, you must close all open windows of your Web browser using the standard window **Close**  button. (On an Apple computer running the OS X operating system, you must also quit the browser.)

## Kualii Financial System (KFS) Modules

This section of the guide presents instructions for the following modules of the Kualii Financial System, listed here alphabetically:

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>• <b>Capital Assets Management</b> [page 24]</li> <li>• <b>Cashiering</b> [below on this page]</li> <li>• <b>Disbursement Vouchers (DV/DVQE)</b> [page 20]</li> <li>• <b>eStatement</b> [page 18]</li> <li>• <b>General Budget Change</b> [page 24]</li> <li>• <b>Internal Billing</b> [page 24]</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Journal Vouchers (JVs)</b> [page 20]</li> <li>• <b>Payroll Expense Transfer &amp; Effort Certification</b> [page 17]</li> <li>• <b>Procurement Card Reallocation</b> [page 12]</li> <li>• <b>Purchasing - Accounts Payable (USC eMarket)</b> [page 13]</li> <li>• <b>SPA Budget Reallocation</b> [page 26]</li> </ul> |
|--|---|

### Cashiering

Follow these instructions to complete the **Cashiering** tab on the User Access Request form. This tab is used to add or remove access privileges that enable a user to submit or approve any of the following types of Cashiering eDocs: *Advance Deposit*, *Cash Receipt*, or *Credit Card Receipt*. When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

#### Instructions for the Add Access section

1. Use the *Access Type* drop-down list to specify whether this user will be assigned the role of a **Preparer** or an **Approver** for the eDoc types you will specify in the next step. A *Preparer* can initiate and submit a Cashiering deposits eDoc, whereas an *Approver* is authorized to approve Cashiering eDocs that have been submitted by other users. The use of the Approver role varies depending on the needs of each department.
2. Select the check-box of each type of Cashiering eDoc for which this user should be granted access privileges.
3. If applicable for your school or department, use the *Workgroup* drop-down list to select the workgroup with which this user will be associated. (A workgroup designation is currently needed only for Keck School of Medicine and the USC Bookstore.)
4. Use the *Campus* drop-down list to select the campus where this user works: *UPC* or *HSC*. (If the user works at a site that is not located on either campus, select *UPC*.)
5. Optionally, use the *Request Explanation* field (or the *Explanation of User Access Request* text box) to enter brief instructions or comments, such as the reason why the applicant needs the access you are requesting.
6. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.

#### Instructions for the Delete Access section

1. Select the check-box of each type of Cashiering eDoc for which you want to remove existing access privileges for this user.
2. If applicable for your school or department, use the *Workgroup* drop-down list to select the workgroup with which this user is associated. (A workgroup designation is currently needed only for Keck School of Medicine and the USC Bookstore.)

3. Use the *Campus* drop-down list to select the campus where this user works: *UPC* or *HSC*. (If the user works at a site that is not located on either campus, select *UPC*.)
4. Optionally, use the *Request Explanation* field (or the *Explanation of User Access Request* text box) to enter brief instructions or comments, such as the reason why you are requesting that this user's access be removed.
5. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.

## Procurement Card Reallocation

This section presents instructions for completing the **Procurement Card Reallocation** tab on the User Access Request form. This tab is used to add or remove access privileges that enable a user to reallocate procurement card transactions from a specific card's default account number and object code to other account numbers and object codes.

A user can be authorized as a reallocator for the 10-digit Organization Code of a single procurement card, or for a group of Organization Codes that all start with the same 5- or 7-digit "mask," thus enabling that user to reallocate transactions for cards associated with any of those Organization Codes.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for the Add Access section

1. Use the *Access Type* drop-down list to specify whether this user will be assigned the role of a **Reviewer**, an **Approver**, or both.
  - A *Reallocator Reviewer* is authorized to redistribute procurement card transaction amounts from the card's default account and object code to other accounts and object codes.
  - A *Reallocator Reviewer Approver* typically reviews and approves the procurement card transaction reallocations that have been submitted by other users.
2. In the *Organization Code* field, enter a complete or partial Organization Code, according to the type of reallocation access you are requesting for the applicant:
  - To request authorization for the user to reallocate transactions for all procurement cards that have default accounts belonging to a particular Organization Code, enter the entire 10-digit Organization Code.
  - To request authorization that will enable the applicant to reallocate transactions on all procurement cards with Organization Codes that begin with the same digits, enter just that 5- or 7-digit "mask." (Naturally, there are more cards associated with a 5-digit mask than with a 7-digit mask.) Enter only digits; do not include an asterisk wildcard character.

If you entered an individual 10-digit Organization Code, the *Organization Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen. (Also note that this tab includes an **Import file** link that you can use to import multiple Organization Codes at once. For instructions, see **Importing Multiple Lines of Data** on page 6.)

3. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.

4. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the Procurement Card Reallocation access changes you are requesting.

#### **Instructions for the *Delete Access* section**

1. In the *Organization Code* field, enter a complete or partial Organization Code, according to the type of reallocation access that should be deleted for the applicant:
  - To remove the user's authorization to reallocate transactions for all procurement cards that have default accounts belonging to a particular Organization Code, enter the entire 10-digit Organization Code.
  - To remove the user's authorization to reallocate transactions on all procurement cards with Organization Codes that begin with the same digits, enter just that 5- or 7-digit "mask." (Naturally, there are more cards associated with a 5-digit mask than with a 7-digit mask.) Enter only digits; do not include an asterisk wildcard character.

If you entered an individual 10-digit Organization Code, the *Organization Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the Procurement Card Reallocation access deletion you are requesting for the applicant.

### **Purchasing - Accounts Payable**

This section presents instructions for completing the **Purchasing - Accounts Payable** tab on the User Access Request form. This tab is used to add or remove assigned user roles, which control the activities that a given user can perform in the **USC eMarket** system. When you are ready to submit the User Access Request eDoc, proceed to ***Submitting Your User Access Request eDoc*** on page 7.

**NOTE:** If you are requesting changes to a user's already-assigned USC eMarket roles and permissions, be sure to complete **both** sections of this tab as needed to request (1) the addition of new access information (e.g., a different assigned department; different or additional visible departments; and different or additional role type and threshold), and (2) deletion of any access information that should no longer in place for this user.

#### **Instructions for the *Add USC eMarket Role* section**

Complete all applicable fields in this section of the **Purchasing - Accounts Payable** tab to request new or additional USC eMarket roles and permissions for the applicant.

1. In the *Assigned Department* field, enter the complete 10-digit Department Organization Code for the department with which this user's USC eMarket transaction documents will be identified. (Each USC eMarket user can have only one assigned department. For an explanation of this code, see page 3.)
2. Although a user will automatically be able to view USC eMarket transaction documents that he/she initiates, access to view transaction documents initiated by others must be requested by specifying the departments whose transaction documents will be "visible" for the applicant. In the *Visible Departments* text box, enter the 10-digit Department Organization Code of the applicant's assigned department and any additional departments for which he/she should be given access to view USC eMarket transaction documents. Be sure to type a semicolon (;) and a space after each

code that you enter (e.g., 1234567891; 1234567892; etc.). No other fields on this tab need to be completed if you are only specifying more visible departments to be added to those previously assigned for this user.

3. Use the *Role* drop-down list to specify a USC eMarket role that you want to assign to this user, or for which you want to request a change to his/her currently assigned approval settings:
    - **eShopper** – Users with this role can place items in a shopping cart, but must assign the cart to an eRequisitioner for submittal. They can also enter Receiving information to confirm receipt of a delivery. (Do not assign this role to a user with the eRequisitioner role; giving both roles to one user can cause system conflicts, and is unnecessary because an eRequisitioner has all the permissions of an eShopper.)
    - **eRequisitioner** – Users with this role can add items to a shopping cart; enter Object Codes, Account Numbers, and delivery information; submit requisitions for approval; and enter Receiving information to confirm receipt of a delivery. (If you are requesting assignment of the eRequisitioner role to a user who already has the eShopper role, be sure to also request removal of the eShopper role for this user by completing the *Delete USC eMarket Role* section (see page 15). Giving both roles to one user can cause system conflicts, and is unnecessary because an eRequisitioner has all the permissions of an eShopper.)
    - **Approvers** – Users with an Approver role can review requisitions, evaluate whether they are appropriate and allowable, provide formal approval, and also facilitate resolution of invoice exceptions. For each set of specified departments, you can assign one of the following Approver roles to the applicant:
      - **eFinancial Approver (Shared)** – one of several users who are each authorized to provide approval of certain dollar amounts when only one approval is required.
      - **eFinancial Approver (Sequential)** – one of several users who will be required to provide up to three consecutive approvals of certain dollar amounts.
      - **eSpecial Account Approver** – authorized to give optional additional approval beyond the eFinancial Approver.
      - **eInvoice Exception Approver** – authorized to approve invoices that cannot be paid due to pricing, quantity, or receipt exceptions.
    - **eReceiver** – Users with this role are authorized only to enter Receiving information to confirm receipt of a delivery. Because the eShopper and eRequisitioner roles are authorized to perform receiving duties, it is redundant to assign the eReceiver role to a user with one of those roles.
- NOTE:** Other fields will be displayed or hidden in this section of the **Purchasing - Accounts Payable** tab depending on your selection in the *Role* drop-down list. For the remaining steps of this procedure, if a particular field is not shown for the role you selected, skip the instructions for that field.
4. Some roles in the USC eMarket are associated with Approval Thresholds, which either (a) place a limit on the purchase amount for which the user can submit a requisition, or (b) require the user to approve any requisition for an amount within a specified range. If appropriate for the role you are assigning, the *Approval Threshold(\$)* drop-down list is displayed so that you can specify one of the following:
    - For the eRequisitioner role, select the maximum dollar amount for which the user will be permitted to submit requisitions without requiring further approval. Requisitions for amounts that exceed the user's specified Approval Threshold will be routed to the eFinancial Approver level for the Account Numbers utilized on the user's requisition. Note

that if you select “None” as the approval threshold, you can skip step 5 and proceed to step 6 because no accounts or Organization Codes have to be specified.

- For an eFinancial Approver or an eSpecial Account Approver, select the dollar range denoting the purchase amounts for which the user will be required to review and approve requisitions.
5. If appropriate for the role you are assigning, the *Access To* drop-down list and the *Accounts (or Masks)/Organization Codes* text box will be displayed so that you can specify the accounts for which the user will have approval access in the USC eMarket.
    - a. In the *Access To* drop-down list, select the type of codes that you will enter in the *Accounts (or Masks)/Organization Codes* text box:
      - Accounts (or Masks)
      - Organization Codes
    - b. In the *Accounts (or Masks)/Organization Codes* text box, enter the appropriate type of data, according to the option you selected in the *Access To* drop-down list. Be sure to type a semicolon (;) and a space after each Account Number or code that you enter:
      - If you chose “Accounts (or Masks),” enter the 10-digit Account Numbers for which the applicant should have access in the USC eMarket, **or** the Account “masks” (4- or 6-digit strings ending with asterisks; e.g., 5348\*) representing those accounts. Make certain that any Account mask you are entering here ends with an asterisk and does not apply to accounts outside of Organization Codes for which the applicant is authorized.
      - If you chose “Organization Codes,” enter the Organization Codes representing all accounts for which the applicant should have access in the USC eMarket.

Note that this section of the **Purchasing - Accounts Payable** tab includes its own **Import file** link in the upper right-hand corner. This link gives you the option of populating the *Accounts (or Masks)/Organization Codes* text box by importing multiple Account Numbers (or 4- or 6-digit masks), **or** Organization Codes from an Excel file, to be associated with the eMarket role you selected in step 3. Be sure that your selection in the *Access To* drop-down list matches the type of data that you are importing. For instructions on importing data, see **Importing Multiple Lines of Data** on page 6.

6. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
7. Repeat steps 3 through 6 as needed to request the addition of other USC eMarket roles and permissions for this applicant.
8. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the USC eMarket access changes you are requesting for the applicant.

### **Instructions for the Delete USC eMarket Role section**

For this section of the **Purchasing - Accounts Payable** tab, you should complete only those fields in which you want to remove existing USC eMarket roles and permissions for the applicant.

1. To request the deletion of the currently assigned department with which this user’s USC eMarket transaction documents are identified, complete the *Assigned Department* field by entering the full 10-digit Department Organization Code for that department. Complete the corresponding field in the *Add USC eMarket Role* section of this tab if you need to specify a new assigned

department for the applicant. (Each USC eMarket user must have a single assigned department. For an explanation of this code, see page 3.)

2. If you want to remove the applicant's currently assigned permission to view eMarket transaction documents associated with any specific departments, enter the 10-digit Department Organization Codes for those departments in the *Visible Departments* text box. Be sure to type a semicolon (;) and a space after each code that you enter (e.g., 1234567891; 1234567892; etc.).
3. If you want to remove an already-assigned USC eMarket role for the applicant, or if you want to delete the currently assigned approval settings for that role, use the *Role* drop-down list to specify the assigned USC eMarket role in question.

**NOTE:** Other fields will be displayed or hidden in this section of the **Purchasing - Accounts Payable** tab depending on which role you selected in the drop-down list. For the remaining steps of this procedure, if a particular field is not shown for the role you selected, skip the instructions for that field.

4. If appropriate for the role you have selected in the *Role* drop-down list, the *Approval Threshold(\$)* drop-down list will be displayed so that you can specify one of the following:
  - For the eRequisitioner role, select the maximum approval amount that you want to delete.
  - For an eFinancial Approver or eSpecial Account Approver, select the required-approval range that you want to delete.
5. If appropriate for the role you have specified, the *Access To* drop-down list and the *Accounts (or Masks)/Organization Codes* text box will be displayed so that you can specify accounts for which the user will no longer have approval access in the USC eMarket.
  - a. In the *Access To* drop-down list, select the type of codes that you will enter in the *Accounts (or Masks)/Organization Codes* text box:
    - Accounts (or Masks)
    - Organization Codes
  - b. In the *Accounts (or Masks)/Organization Codes* text box, enter the appropriate type of data, according to the option you selected in the *Access To* drop-down list. Be sure to type a semicolon (;) and a space after each Account Number or code that you enter:
    - If you chose "Accounts (or Masks)," enter the 10-digit Account Numbers for which you want to remove the applicant's access in the USC eMarket, **or** the Account "masks" (4- or 6-digit strings ending with asterisks; e.g., 5348\*) representing those accounts. Make certain that any Account mask you are entering here ends with an asterisk and does not apply to accounts outside of Organization Codes for which the applicant is authorized.
    - If you chose "Organization Codes," enter the Organization Codes representing all accounts for which you want to remove the applicant's access in the USC eMarket. Note that this user will no longer be able to view eMarket transaction documents for any of the accounts associated with the Organization Codes you are specifying.

Note that this section of the **Purchasing - Accounts Payable** tab includes its own **Import file** link in the upper right-hand corner. This link gives you the option of populating the *Accounts (or Masks)/Organization Codes* text box by importing multiple Account Numbers (or 4- or 6-digit masks), **or** Organization Codes from an Excel file, to be associated with the eMarket role you selected in step 3. Be sure that your selection in the *Access To* drop-down list matches the type of data that you are importing. For instructions on importing data, see **Importing Multiple Lines of Data** on page 6.



6. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
7. Repeat steps 3 through 6 as needed to request the removal of other USC eMarket roles and permissions for this applicant.
8. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the USC eMarket access deletion you are requesting for the applicant.

### Payroll Expense Transfer & Effort Certification

This section presents instructions for completing the **Payroll Expense Transfer & Effort Certification** tab on the User Access Request form. This tab enables you to add or remove the assigned user roles that control which tasks a user can perform with the Payroll Expense Transfer (PET) and Effort Certification (EC) eDocs. The PET eDoc is designed for making retroactive credit and debit adjustments to accounts against which payroll expenses have been charged. The EC eDoc is used to provide an after-the-fact method of accounting for the percentage of effort for employees who are paid in full or in part, or through cost sharing, from controlled funds that are part of a sponsored project agreement.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

#### Instructions for adding or deleting Payroll Expense Transfer and Effort Certification roles

1. In the *Department Role* drop-down list, select the *USC Department* role that you want to add or delete for the applicant.
  - **Payroll Transfer and View** – Users with this role can initiate PET eDocs to perform payroll expense transfers on any account for which they have access rights in KFS. Bear in mind that users with this role will be able to see sensitive payroll information for all accounts to which they have access rights.
  - **Departmental Approval and To Line Approval** – These two roles enable you to designate a department’s authorized financial approver for PET eDocs.
    - The *Departmental Approval* role pertains to PET approval for the department that owns the “From” account originally charged for the salary in question.
    - The *To Line Approval* role pertains to PET approval for the department that owns the “To” account to which the charge is being transferred.

For PET eDocs, the same person should be assigned both the *Departmental Approval* and *To Line Approval* roles. It is important for your department’s financial approver to have the *To Line* approval authority in order to ensure that other departments cannot charge your account without your approval.

- **Optional Departmental Pre-Approval** – As indicated by its name, this PET role is optional. It is available to departments who want an additional level of review before PET transactions go to the department’s authorized financial approver.
  - **Effort Certification Reviewer** – Users with this role are responsible for overseeing effort certification, following up on delinquent certifications, assisting with the enforcement of effort certification policy, and assigning Preparers to Certifiers. (The *Preparer* and *Certifier* roles are derived automatically rather than being assigned.)
2. In the *Add/Delete Role* drop-down list, select the appropriate option to indicate whether you are adding or removing the role you specified in the *Department Role* drop-down list.

3. For the *Organization Code* field, proceed as follows:
  - Leave this field blank if you are requesting the addition or deletion of the *Payroll Transfer and View* role, or the *Effort Certification Reviewer* role.
  - If you are requesting the addition or deletion of a PET approval role, you must enter a 10-digit organization code, or a 5- or 7-digit organization code “mask,” for which the authorized financial approver should receive PET requests. If you are specifying a mask, be sure to enter it as a 5- or 7-digit string ending with an asterisk (e.g., 63547\* or 9837463\*).
4. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
5. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the PET access changes you are requesting for the applicant.

### eStatement




This section presents instructions for completing the **eStatement** tab on the User Access Request form, which enables you to take any of the following actions:

- Update system records to show the applicant has a different supervisor than the one currently on file.
- Update system records to show the applicant’s default supervisor listed in the Workday system.
- Add, change, or delete another user who is designated to act as a proxy for the applicant in taking action on eStatements.
- Add or remove Business Office Reviewer (BOR) rights for the applicant in relation to one 10-digit Organization Code or a group of Organization Codes that start with the same 5- or 7-digit “mask.”

When completing this tab, note that you can use the optional *Explanation of User Access Request* text box to enter brief instructions or comments about the eStatement-related access changes you are requesting for the applicant.

When you are ready to submit the User Access Request eDoc, proceed to ***Submitting Your User Access Request eDoc*** on page 7.

### Instructions for the *Change Supervisor* section

1. Enter the first and last names of the applicant’s *Current Supervisor*, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page.
2. Enter the first and last names of the applicant’s *New Supervisor*, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page.
3. Enter the first and last names of the applicant’s default supervisor listed in Workday, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page. (In Workday, perform a search for the name of the employee, and his/her supervisor’s name will be shown in parentheses at the end of the listing of the employee’s job information.)

**NOTE:** You must enter the names and ID numbers for ALL THREE SETS OF FIELDS: *Current Supervisor*, *New Supervisor*, and *Default Supervisor from Workday*.

### **Instructions for the Proxy section**

In the *Proxy User Action* drop-down list, select the type of action you want to request, and complete other fields as detailed here:

- **Add Proxy User** – Complete only the *New Proxy First Name*, *New Proxy Last Name*, and *New Proxy USC ID Number* fields.
- **Change Proxy User**
  - a. Enter the first and last names of the applicant's *Current Proxy User*, as well as his or her 10-digit USC ID number, in the designated fields.
  - b. Enter the first and last names of the applicant's *New Proxy User*, as well as his or her 10-digit USC ID number, in the designated fields.
- **Delete Proxy User** – Complete only the *Current Proxy First Name*, *Current Proxy Last Name*, and *Current Proxy USC ID Number* fields.

### **Instructions for the Business Office Reviewer (BOR) section**

Complete the appropriate section to add or delete Organization Code-specific Business Office Reviewer access privileges for the applicant, as described below. (Also note that this section of the **eStatement** tab includes an **Import file** link that you can use to import multiple Organization Codes at once when adding or deleting access. For instructions, see **Importing Multiple Lines of Data** on page 6.)


- **Add BOR Access**
  - a. In the *Organization Code* field, enter a complete 10-digit Organization Code for which the applicant should be granted access, **or** enter a 5- or 7-digit “mask” to give the applicant access to all Organization Codes that begin with those same digits. Enter only digits; do not include an asterisk wildcard character.
  - b. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information. If you entered an individual 10-digit Organization Code, the *Organization Name* field will automatically be populated with information corresponding to your entry.
  - c. Repeat steps *a* and *b* as needed to request that the applicant be granted access privileges for any other Organization Codes.
- **Delete BOR Access**
  - a. In the *Organization Code* field, enter a complete 10-digit Organization Code for which the applicant's access should be removed, **or** enter a 5- or 7-digit “mask” to delete the applicant's access to all Organization Codes that begin with those same digits. Enter only digits; do not include an asterisk wildcard character.
  - b. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information. If you entered an individual 10-digit Organization Code, the *Organization Name* field will automatically be populated with information corresponding to your entry.
  - c. Repeat steps *a* and *b* as needed to request removal of the applicant's access for any other Organization Codes.

## Journal Vouchers (JVs)


Follow the instructions in this section to complete the **Journal Vouchers (JVs)** tab on the User Access Request form. This tab is used to add or remove access privileges that enable a user to prepare and/or approve entries for specific Journal Voucher numbers. (Also note that this tab includes an **Import file** link that you can use to import multiple JV numbers at once when you are adding or deleting access. For instructions, see **Importing Multiple Lines of Data** on page 6.)

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for the Add Access section

1. Select the check-box (or boxes) that correspond to the type of access that the applicant should be granted for the Journal Voucher number that you are specifying in the same row. (If you are using the **Import file** option, your selection will apply to all of the JV numbers that you import.)
2. In the *JV Number* field, enter the 3-digit Journal Voucher number for which the applicant should be granted access. If you need to search for the appropriate department code, click the lookup icon  next to the *JV Number* field to access the **Journal Voucher Number Lookup** page.
3. Click the  button in the *Actions* column. The *JV Description* field will automatically be populated with information corresponding to your entry in the *JV Number* field, and the line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
4. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the JV access changes you are requesting for the applicant.

### Instructions for the Delete Access section

1. In the *JV Number* field, enter the 3-digit Journal Voucher number for which the applicant's access should be deleted. If you need to search for the appropriate department code, click the lookup icon  next to the *JV Number* field to access the **Journal Voucher Number Lookup** page.
2. Click the  button in the *Actions* column. The *JV Description* field will automatically be populated with information corresponding to your entry in the *JV Number* field, and the line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the JV access deletion you are requesting for the applicant.

## Disbursement Vouchers (DV/DVQE)

Follow the instructions in this section to complete the **Disbursement Vouchers (DV/DVQE)** tab on the User Access Request form. This tab is used to add or remove user roles that control the applicant's ability to initiate, review, and approve Disbursement Vouchers (DVs) and Disbursement Voucher Quick Expense forms (DVQEs), which respectively replace the WebBA Check Request and Quick Expense functionality.

Note that you can use the optional *Explanation of User Access Request* text box to enter comments about the DV or DVQE access changes you are requesting for the applicant. When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

**Instructions for the *Add DV & DVQE Access* section**

Complete all applicable fields in this section of the **Disbursement Vouchers** tab to request new or additional DV/DVQE roles and permissions for the applicant.

1. Use the *Role* drop-down list to specify a DV/DVQE role that you want to assign to this user, or for which you want to request a change to his/her currently assigned approval settings:
  - **DV Initiator** – Users with this role can initiate and submit DV eDocs to request payments to suppliers. (By default, all USC employees are assigned the permission needed to initiate DVQE eDocs.)
  - **Account Delegates** – The default Financial Approver role is assigned to the Account Fiscal Officer, but the following roles are used to authorize other users as delegate approvers. Delegate approvers can be authorized for individual Account Numbers or Organization Codes, or for Account “masks” (strings of digits ending with an asterisk, representing all Account Numbers that begin with those same digits).
    - **Primary Account Delegate DV/DVQE** – This role is used to authorize a user as a primary delegate approver for the use of funds from the account specified in the DV or DVQE eDoc. Note that only one primary account delegate can be specified.
    - **Secondary Account Delegate DV/DVQE** – This role is used to authorize a user as a secondary delegate approver for the use of funds from the account specified in the DV or DVQE eDoc. Multiple users can be authorized as secondary account delegates.
  - **Organization Reviewers** – These roles are used when it is desired to include an additional review step in the workflow for DV and DVQE eDocs associated with a particular Organization Code. The optional Organization Review will occur after the eDoc in question has received Financial Approval, and just before it is routed to Disbursement Control and Accounts Payable for final approval and payment.
    - **Organization Reviewer DV** – Users with this role are authorized to perform the optional step of reviewing DV eDocs associated with a specified Organization Code.
    - **Organization Reviewer DVQE** – Users with this role are authorized to perform the optional step of reviewing DVQE eDocs associated with a specified Organization Code.
  - **Special Account Approver DV/DVQE** – Users with this role are authorized to give optional additional approval beyond the Financial Approver for DV or DVQE eDocs associated with individual Account Numbers or Organization Codes, or with Account “masks” (strings of digits ending with an asterisk, representing all Account Numbers that begin with those same digits).

**NOTE:** Other fields will be shown or hidden in this section of the **Disbursement Vouchers** tab depending on which role you selected in the drop-down list. For the remaining steps of this procedure, if a particular field is not shown for the role you selected, skip the instructions for that field.

2. Some DV and DVQE roles are associated with Approval Thresholds, which require the user to approve any request for an amount that falls within a specified range. If appropriate for your selection in the *Role* drop-down list, the *Approval Threshold(\$)* drop-down list is displayed so that you can select the dollar range denoting the amounts for which the user will be required to review and approve the DV or DVQE request.
3. If appropriate for the role you are assigning, the *Access To* drop-down list and the *Accounts (or Masks)/Organization Codes* text box will be displayed so that you can specify the accounts for which the user will have review and approval access.
  - a. In the *Access To* drop-down list, select the type of codes that you will enter in the *Accounts (or Masks)/Organization Codes* text box:

- Accounts (or Masks)
- Organization Codes

**NOTE:** If you selected one of the Organization Reviewer roles in the *Role* drop-down list, then “Organization Codes” will automatically be selected for you in the *Access To* drop-down list. If you change this default selection, an error message will be displayed because only Organization Codes can be used to assign access to the Organization Reviewer roles.

- b. In the *Accounts (or Masks)/Organization Codes* text box, enter the appropriate type of data, according to the option you selected in the *Access To* drop-down list. Be sure to type a semicolon (;) and a space after each Account Number or Organization Code that you enter:
  - If you chose “Accounts (or Masks),” enter the 10-digit Account Numbers for which the applicant should have access, **or** the Account “masks” (4- or 6-digit strings ending with asterisks; e.g., 5348\*) representing those accounts. Make certain that any Account mask you are entering here ends with an asterisk and does not apply to accounts outside of Organization Codes for which the applicant is authorized.
  - If you chose “Organization Codes,” enter the Organization Codes representing all accounts for which the applicant should have access.
4. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
5. Repeat steps 1 through 4 as needed to request the addition of other DV roles and permissions for this applicant.
6. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the DV or DVQE access changes you are requesting for the applicant.

### **Instructions for the *Delete DV & DVQE Access* section**

For this section of the **Disbursement Vouchers** tab, you should complete only those fields in which you want to remove existing DV/DVQE roles and permissions for the applicant.

1. If you want to remove an already-assigned role for the applicant, or if you want to delete the currently assigned approval settings for that role, use the *Role* drop-down list to specify the assigned DV/DVQE role in question.




**NOTE:** Other fields will be shown or hidden in this section of the **Disbursement Vouchers** tab depending on which role you selected in the drop-down list. For the remaining steps of this procedure, if a particular field is not shown for the role you selected, skip the instructions for that field.

2. If appropriate for your selection in the *Role* drop-down list, the *Approval Threshold(\$)* drop-down list will be displayed so that you can select the required approval range that you want to delete.
3. If appropriate for the role you are assigning, the *Access To* drop-down list and the *Accounts (or Masks)/Organization Codes* text box will be displayed so that you can specify accounts for which the user will no longer have review and approval access.
  - a. In the *Access To* drop-down list, select the type of codes that you will enter in the *Accounts (or Masks)/Organization Codes* text box:
    - Accounts (or Masks)
    - Organization Codes

**NOTE:** If you selected one of the Organization Reviewer roles in the *Role* drop-down list, then “Organization Codes” will automatically be selected for you in the *Access To* drop-down list. If you change this default selection, an error message will be displayed because only Organization Codes can be used to assign access to the Organization Reviewer roles.

- b. In the *Accounts (or Masks)/Organization Codes* text box, enter the appropriate type of data, according to the option you selected in the *Access To* drop-down list. Be sure to type a semicolon (;) and a space after each Account Number or Organization Code that you enter:
  - If you chose “Accounts (or Masks),” enter the 10-digit Account Numbers for which you want to remove the applicant’s access, **or** the Account “masks” (4- or 6-digit strings ending with asterisks; e.g., 5348\*) representing those accounts. Make certain that any Account mask you are entering here ends with an asterisk and does not apply to accounts outside of Organization Codes for which the applicant is authorized.
  - If you chose “Organization Codes,” enter the Organization Codes representing all accounts for which you want to remove the applicant’s access. Note that this user will no longer be able to view DV or DVQE eDocs for any of the accounts associated with the Organization Codes you are specifying.
4. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
5. Repeat steps 1 through 4 as needed to request the addition of other DV roles and permissions for this applicant.
6. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the DV or DVQE access changes you are requesting for the applicant.

#### **Instructions for the Change DV/DVQE Supervisor section**

1. Enter the first and last names of the applicant’s *Current Supervisor*, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page.
2. Enter the first and last names of the applicant’s *New Supervisor*, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page.
3. Enter the first and last names of the applicant’s default supervisor listed in Workday, as well as his or her 10-digit USC ID number, in the designated fields. Click the adjacent lookup icon  if you need to access the **Person Lookup** page. (In Workday, perform a search for the name of the employee, and his/her supervisor’s name will be shown in parentheses at the end of the listing of the employee’s job information.)

**NOTE:** You must enter the names and ID numbers for ALL THREE SETS OF FIELDS: *Current Supervisor*, *New Supervisor*, and *Default Supervisor from Workday*.

4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the DV or DVQE access changes you are requesting for the applicant.

### Internal Billing

The **Internal Billing** tab on the User Access Request form is used to add or remove the user role required to work with the Internal Billing Requisition eDoc. The IBR eDoc enables authorized users in a university department to requisition goods or services from a designated Service Center.

To complete this tab, select the appropriate option in the drop-down list to indicate whether you want to add or delete the IBR Document Initiator role. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the Internal Billing access changes you are requesting for the applicant.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### General Budget Change

The **General Budget Change** tab on the User Access Request form is used to add or remove the user role required to work with the General Budget Change eDoc. The GBC eDoc enables authorized users to submit changes throughout the fiscal year to the annual budget amounts set for their departments by the Office of Budget and Planning.

To complete this tab, select the appropriate option in the drop-down list to indicate whether you want to add or delete the GBD Departmental User role. Optionally, use the *Explanation of User Access Request* text box to enter brief instructions or comments about the General Budget Change access changes you are requesting for the applicant.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Capital Assets Management

Follow the instructions in this section to complete the **Capital Assets Management** tab on the User Access Request form. This tab enables you to add or remove access privileges that allow a user to view account-specific information about assets (i.e., equipment) in the Capital Assets Management System (CAMS).

When adding or deleting access, you can specify complete, individual 10-digit Account Numbers or 10-digit Organization Codes, **or** you can specify Account or Organization Code “masks” (strings of digits ending with an asterisk, representing all Account Numbers or Organization Codes that begin with those same digits). The account-level access granted by means of Organization Codes applies only to CAMS data.

**NOTE:** If a Kualu user has access privileges to use KFS Inquiries and the Business Intelligence/Cognos General Ledger reports (discussed on page 32), then granting that user account-specific access for CAMS will also enable him or her to view financial data for the same accounts in inquiries and BI reports.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7. If an error message is shown, indicating that you have exceeded the allowable number of characters, then simply submit a second User Access Request eDoc for any Account Numbers and/or Organization Codes that could not be included.

### Instructions for the Add Account Level Access section

This section of the **Capital Assets Management** tab offers you a great deal of flexibility when requesting the addition of account-level access to CAMS data. You can enter any combination of Account Numbers,



Account “masks,” Organization Codes, and Organization Code masks that will best enable you to specify all accounts for which the applicant should be granted access rights.

**NOTE:** The words “KFS-SEC ETL Default” in parentheses on this tab refer to the fact that any account level access added here may give the applicant access to various other parts of the financial system, depending on which user roles he or she has been assigned.

1. Use the *Access to Account Numbers or Account Masks* field to enter the complete 10-digit Account Numbers of any individual accounts for which the applicant should be granted access, **or** to enter Account “masks” (1- to 9-digit strings ending with asterisks; e.g., 6\* or 5348\*) if you want to give him/her access to all Account Numbers that begin with those same digits. Be sure to type a semicolon (;) and a space after each Account Number or mask that you enter.
2. If you want to request that the applicant be granted access to all accounts associated with one or more Organization Codes, use the *Access to Organization Codes or Organization Code Masks* field to enter either the complete 10-digit Organization Codes **or** the 5-, 7-, or 9-digit Organization Code “masks” representing all Organization Codes that begin with those same digits. Be sure to end each mask with an asterisk (\*), and type a semicolon (;) and a space after each Organization Code or mask that you enter.
3. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the CAMS access changes you are requesting for the applicant.

#### **Instructions for the *Delete Account Level Access* section**

This section of the **Capital Assets Management** tab offers you a great deal of flexibility when requesting the removal of account-level access to CAMS data. You can enter any combination of Account Numbers, Account masks, Organization Codes, and Organization Code masks that will best enable you to specify all accounts for which the applicant’s current access rights should be deleted.

**NOTE:** The words “KFS-SEC ETL Default” in parentheses on this tab refer to the fact that any account level access deleted here may also impact the applicant’s access to various other parts of the financial system, depending on which user roles he or she has been assigned.

1. Use the *Access to Account Numbers or Account Masks* field to enter the complete 10-digit Account Numbers of any individual accounts for which the applicant’s access rights should be deleted, **or** to enter Account “masks” (1- to 9-digit strings ending with asterisks; e.g., 6\* or 5348\*) if you want to remove his/her access to all Account Numbers that begin with those same digits. Be sure to type a semicolon (;) and a space after each Account Number or mask that you enter.
2. If you want to request the removal of the applicant’s access to all accounts associated with one or more Organization Codes, use the *Access to Organization Codes or Organization Code Masks* field to enter either the complete 10-digit Organization Codes **or** the 5-, 7-, or 9-digit Organization Code “masks” representing all Organization Codes that begin with those same digits. Be sure to end each mask with an asterisk (\*), and type a semicolon (;) and a space after each Organization Code or mask that you enter.
3. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the CAMS access changes you are requesting for the applicant.

## SPA Budget Reallocation

The **SPA Budget Reallocation** tab on the User Access Request form is used to add or remove user roles required in order to submit the SPA Budget Reallocation (BR) eDoc. The SPA BR eDoc enables authorized users in a university department to reallocate funds between object codes within one or more account numbers associated with the same sponsored award. To complete this tab, follow these steps:

1. In the *Add/Delete Role* drop-down list, select the appropriate option to indicate whether you are requesting the addition or deletion of a SPA BR role for the applicant.
2. Use the *Role* drop-down list to specify the SPA BR role that should be added or deleted.
3. The *Organization Code* field is required for a SPA BR Department Approver I or II role:
  - If you are adding or removing departmental approval rights for all accounts that belong to one specific Organization Code, enter the complete 10-digit Organization Code.
  - If you are adding or removing departmental approval rights for all accounts that belong to a “roll-up” group of Organization Codes that begin with the same 5 or 7 digits, enter that 5- or 7-digit string ending with an asterisk (\*).

If you entered an individual 10-digit Organization Code, the *Organization Code Name* field will automatically be populated with the name corresponding to your entry when you press the TAB key or click elsewhere on the screen.

4. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
5. Use the *Explanation of User Access Request* text box to enter comments about the SPA BR access changes you are requesting. If you are requesting the SPA BR Department Approver I or II role, be sure to specify whether the role should be granted to the applicant as an individual or should be applied to a workgroup. In other words, your entry should explain whether there are other users who should have that same department approver role for the same Organization Code, and whether they are already in an existing workgroup or if a new workgroup should be created.

## Kuali Enterprise Workflow (KEW) Modules

This section of the guide presents instructions for the Kuali Enterprise Workflow modules of the Kuali system, listed here alphabetically:

- |  |  |
|--|--|
| • <b>Chart of Accounts (COA)</b> [page 29] | • <b>Financial Aid Account (FAA)</b> [page 27]         |
| • <b>Course Scheduling</b> [page 29]       | • <b>General Purpose Workflow</b> [below on this page] |

## General Purpose Workflow

Follow the instructions in this section to complete the **General Purpose Workflow** tab on the User Access Request Document form, which enables you to take any of the following actions:

- Add the applicant to one or more workgroups.
- Delete the applicant from one or more workgroups.
- Request the creation of a new workgroup.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### **Instructions for Adding the Applicant to a Workgroup**

1. In the *Workgroup Name* drop-down list, select a workgroup to which this user should be added.
2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Repeat steps 1 and 2 as needed for other workgroups to which the applicant should be added.
4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the access changes you are requesting for the applicant.

### **Instructions for Deleting the Applicant From a Workgroup**

1. In the *Workgroup Name* drop-down list, select the workgroup from which this user should be removed.
2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Repeat steps 1 and 2 as needed for other workgroups from which the applicant should be deleted.
4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the access changes you are requesting for the applicant.

### **Instructions for Requesting the Creation of a New Workgroup**

1. In the *Workgroup Name* field, type the name of the new workgroup that should be created.
2. Optionally, use the *Workgroup Request Comments* field to enter brief instructions or comments, such as the reason why you are requesting the creation of this new workgroup.
3. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
4. Repeat steps 1 through 3 as needed to request the creation of additional workgroups.
5. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the access changes you are requesting for the applicant.

## **Financial Aid Account (FAA)**

Follow the instructions in this section to complete the **Financial Aid Account** tab, which is used to request access rights for the applicant to review and approve KEW Financial Aid Account (FAA) eDocs. The FAA eDoc is used to request the creation of new financial aid award codes and to specify changes that should be made to existing award codes.

**NOTE:** If the applicant for whom you are submitting this request is **not** employed within the Office of Financial Aid, you can specify only one Financial Aid Account (FAA) role to be added or removed. Submit a separate User Access Request eDoc if you want to add or delete any other FAA roles for this individual.

When you are ready to submit the User Access Request eDoc, proceed to ***Submitting Your User Access Request eDoc*** on page 7.

### **Instructions for adding or deleting Financial Aid Account roles**


1. In the *FAA Role* drop-down list, select the *USC Departments* role or *Financial Aid Department* role that you want to add or delete for the applicant.

- **Roles for USC Departments**
    - **FAA Reviewer** – This role is intended for a fiscal officer who will be responsible for approving financial aid transactions sourced from accounts that he/she oversees, which are associated with the Organization Codes you are specifying in the next section of the **Financial Aid Account** tab.
    - **Optional FAA Reviewer** – Some departments may choose to designate an additional approver to review financial aid transactions before they are approved by a senior fiscal officer. When this User Access Request eDoc is processed, the applicant to whom you are assigning the Optional FAA Reviewer role will be linked to the Organization Codes that you will specify in step 3 below.
  - **Roles for Financial Aid Department**
    - **Financial Aid Workgroup** – This role is reserved for personnel in the Office of Financial Aid who are authorized to approve financial aid transactions.
    - **FAA View All** – Users assigned this role will be given view-only access for any KEW FAA eDoc, regardless of whether they were included in the document’s route path.
    - **Both Financial Aid Workgroup and FAA View All Roles** – This role is intended for someone in the Office of Financial Aid who may need both the authority to approve new KEW FAA eDocs and the capability to view FAA eDocs that were initiated in the past.
2. In the *FAA Role Add/Delete* drop-down list, select the appropriate option to indicate whether you are requesting the addition or removal of the role you specified in the *FAA Role* drop-down list.
  3. If you selected one of the *USC Department* roles in the *FAA Role* drop-down list, complete the *Organization Code* field, as follows. If you selected one of the *Financial Aid Department* roles, skip this step and proceed to step 4.
    - a. In the *Organization Code* field, individually enter each Organization Code or “mask” that you want to associate with the *USC Department* role that you specified in the *FAA Role* drop-down list. You can enter either a complete 10-digit Organization Code **or** a 5- or 7-digit Organization Code “mask” representing all Organization Codes that begin with those same digits. Enter only digits; do not include an asterisk wildcard character.
    - b. Click the  button in the *Actions* column. The *Organization Code Name* field will automatically be populated with the name corresponding to your entry in the *Organization Code* field, and the line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
    - c. Repeat steps *a* and *b* as needed to add all applicable 10-digit Organization Codes **or** 5- or 7-digit Organization Code “masks.”
  4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the FAA role changes you are requesting for the applicant.

## Chart of Accounts (COA)

Follow the instructions in this section to complete the **Chart of Accounts** tab, which is used to request access rights for the applicant to create and submit eDocs with the Chart of Accounts options available on the Workflow Main Menu screen. Using those “KEW-COA” options, authorized users can request the creation of new accounts and specify changes to be made to existing accounts. When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for the Add or Delete User Access section

1. In the *Access Type* drop-down list, select the appropriate option to indicate whether you are requesting the addition or removal of access for the applicant to the department code that you will specify in the following step.
2. In the *Department Code* field, enter the department code for which you are requesting the addition or removal of COA access for the applicant. You can enter only one department code. Note that this is not a numerical Home Department Code; it is a letter code identifying the school or department whose SBO will be responsible for approving the COA eDocs submitted by the applicant. If you need to search for the appropriate department code, click the lookup icon  next to the *Department Code* field to access the **Chart of Accounts Department Lookup** page.
3. Click the  button in the *Actions* column. The *Department Description* field will automatically be populated with information corresponding to your entry, and the line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
4. Repeat steps 1 through 3 as needed to request the addition or removal of access for the applicant to other department codes.
5. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the Chart of Accounts access changes you are requesting for the applicant.

## Course Scheduling

Follow the instructions in this section to complete the **Course Scheduling** tab on the User Access Request Document form, which enables you to take any of the following actions:

- Add the applicant to one or more workgroups.
- Delete the applicant from one or more workgroups.
- Request the creation of a new workgroup.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for Adding the Applicant to a Workgroup

1. In the *Workgroup Name* drop-down list, select a workgroup to which this user should be added.
2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Repeat steps 1 and 2 as needed for any other workgroups to which the applicant should be added.

4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the Course Scheduling access changes you are requesting for the applicant.

#### **Instructions for Deleting the Applicant From a Workgroup**

1. In the *Workgroup Name* drop-down list, select the workgroup from which the user should be removed.
2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Repeat steps 1 and 2 as needed for any other workgroups from which the applicant should be deleted.
4. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the Course Scheduling access changes you are requesting for the applicant.

#### **Instructions for Requesting the Creation of a New Workgroup**

1. In the *Workgroup Name* field, type the name of the new workgroup that should be created.
2. Optionally, use the *Workgroup Request Comments* field to enter brief instructions or comments, such as the reason why you are requesting the creation of this new workgroup.
3. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
4. Repeat steps 1 through 3 as needed to request the creation of additional workgroups.
5. Optionally, use the *Explanation of User Access Request* text box to enter instructions or comments about the Course Scheduling access changes you are requesting for the applicant.

## Account Level, Organization Code Level, Payroll Reporting, and BI Planning & Projections Access

Your ability to use different parts of the Kualo Financial System depends on the Account- and Organization Code-specific access rights that you have been given. You must also be assigned the proper roles in order to perform various functions — such as viewing KFS inquiry results and Business Intelligence/Cognos financial reports, submitting Payroll Expense Transfers, or accessing the Capital Assets Management module — for the Account Numbers and/or Organization Codes to which you have been granted access. The applicant's access rights for specific Account Numbers, Organization Codes, and user roles can be added, changed, or removed by completing the appropriate tabs on the User Access Request form:

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• <b>Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 31]</li> <li>• <b>Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 33]</li> <li>• <b>Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 35]</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)</b> [page 37]</li> <li>• <b>Payroll Business Intelligence Reporting Access</b> [page 38]</li> <li>• <b>BI Planning and Projections (P&amp;P)</b> [page 40]</li> </ul> |
|---|--|

### Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)

The **Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request that the applicant be authorized to view information (a) for *individual* 10-digit Account Numbers, (b) for groups of Account Numbers that all start with the same 4- or 6-digit “mask,” or (c) for *all* Account Numbers. You can also specify Account Numbers to be excluded from Organization Codes or account masks to which the applicant will be granted access.

Note that this tab includes an **Import file** link that you can use to import multiple Account Numbers or masks at once when you are adding access rights. For instructions, see **Importing Multiple Lines of Data** on page 6.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for Adding Access to Individual Account Numbers or to Account Masks

1. In the uppermost section of the **Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:
  - To request that the applicant be granted access to one specific account, enter the complete 10-digit Account Number.
  - To request that the applicant be granted access to all Account Numbers that begin with the same digits, enter that 4- or 6-digit “mask” followed by an asterisk (\*). Bear in mind that there are more Account Numbers associated with a 4-digit mask than with a 6-digit mask. Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 5348\*).
  - To request that the applicant be granted access to ALL accounts at the university, enter just an asterisk (\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the account access changes you are requesting for the applicant.

**NOTE:** When requesting that the applicant be given access to the accounts associated with an account mask, if there are specific account numbers that should be omitted from those to which he/she will have access, be sure to specify them as explained in the next section, *Instructions for Excluding Account Numbers When Adding Account Mask Access*.

### **Instructions for Excluding Account Numbers When Adding Account Mask Access**

Use the following procedure to specify any Account Numbers that should be excluded from the group of Account Numbers belonging to an account mask for which the applicant will be granted access. The applicant will not be able to access the excluded accounts.

1. In the second section of the **Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:
  - To request the exclusion of an individual account from an account mask, enter the complete 10-digit Account Number.
  - To request the exclusion of all accounts that begin with the same six numbers, enter that 6-digit mask followed by an asterisk (\*). Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 534854\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the account access changes you are requesting for the applicant.

### **Instructions for Adding Access to KFS Inquiries and Cognos Reports**

The *Inquiries and Reports: Choose Add Access* section of the **Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request that the applicant be given access to run the General Ledger inquiries available on the KFS Financial Main Menu, and also (optionally) the BI/Cognos GL reports available on the Business Intelligence Portal for KFS.

**NOTE:** In order to run BI/Cognos GL reports, the applicant must also have access to run the KFS inquiries. When a user runs either inquiries or BI/Cognos reports, they will only contain data for those accounts to which he/she has been granted access rights at the Account or Organization Code level. If the applicant has been granted account-specific access for the Capital Assets Management System (discussed on page 24), then he/she will be able to view data for those same accounts in inquiries and BI/Cognos reports.

The *None* option is selected by default. To request that access be added, select another option:

- If you want the applicant to have access to run the KFS inquiries, but not the BI/Cognos GL reports, select the radio button labeled *Inquiries Access Only*.



- If you want to request that the applicant be granted access to run the KFS inquiries *and* the BI/Cognos GL reports, select the radio button labeled *Both Inquiries and Cognos Reports Access*.

Optionally, use the *Explanation of Request* text box to enter comments about the access changes you are requesting for the applicant. If requesting only access for KFS inquiries and BI/Cognos GL reports, and not the addition of any account-specific access rights, you can submit the User Access Request eDoc without completing the rest of the **Add Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab.

### Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)

The **Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request the deletion of the applicant's access rights to view information (a) for *individual* 10-digit Account Numbers, (b) for groups of Account Numbers that all start with the same 4- or 6-digit "mask," or (c) for *all* Account Numbers. You can also specify Account Numbers to be excluded from those for which you are removing his/her access rights.

Note that this tab includes an **Import file** link that you can use to import multiple Account Numbers or masks at once when you are deleting access rights. For instructions, see *Importing Multiple Lines of Data* on page 6.

When you are ready to submit the User Access Request eDoc, proceed to *Submitting Your User Access Request eDoc* on page 7.

### Instructions for Removing Access to Individual Account Numbers or to Account Masks

1. In the uppermost section of the **Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:
  - To request removal of the applicant's access for one specific account, enter the complete 10-digit Account Number.
  - To request removal of the applicant's access for all Account Numbers that begin with the same digits, enter that 4- or 6-digit "mask" followed by an asterisk (\*). Bear in mind that there are more Account Numbers associated with a 4-digit mask than with a 6-digit mask. Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 5348\*).
  - To request removal of the applicant's access to ALL accounts, enter just an asterisk (\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.
2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the account access removal you are requesting for the applicant.

**NOTE:** When requesting removal of the applicant's access to the accounts associated with an account mask, if there are any account numbers to which he/she should still have access, be sure to specify them as explained in the next section, *Instructions for Excluding Account Numbers When Removing Account Mask Access*.

### **Instructions for Excluding Account Numbers When Removing Account Mask Access**

Use this procedure if you want to specify any Account Numbers that should be excluded from the group of accounts belonging to an account mask for which you are requesting removal of the applicant's access. The applicant will still be able to access the excluded accounts.

1. In the second section of the **Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:
  - To request the exclusion of an individual account from an account mask, enter the complete 10-digit Account Number.
  - To request the exclusion of all accounts that begin with the same six numbers, enter that 6-digit mask followed by an asterisk (\*). Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 534854\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the account access removal you are requesting for the applicant.

### **Instructions for Removing Access to KFS Inquiries and Cognos Reports**

The *Inquiries and Reports: Choose Delete Access* section of the **Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request the removal of the applicant's access to run the General Ledger inquiries available on the Financial Main Menu in Kualu, and also the BI/Cognos GL reports available on the Business Intelligence Portal for KFS.

**NOTE:** In order to run BI/Cognos GL reports, the applicant must also have access to run the KFS inquiries. When a user runs either inquiries or BI/Cognos reports, they will only contain data for those accounts to which he/she has been granted access rights at the Account or Organization Code level. If the applicant has been granted account-specific access for the Capital Assets Management System (discussed on page 24), then he/she will be able to view data for those same accounts in inquiries and BI/Cognos reports.

The *None* option is selected by default. To request that access be removed, select another option:

- Select the radio button labeled *Cognos Reports Access Only* to request removal of the applicant's access to run the BI/Cognos GL reports, while leaving him/her the ability to run the KFS inquiries.
- To request removal of the applicant's access to run the KFS inquiries *and* the BI/Cognos GL reports, select the radio button labeled *Both Inquiries and Cognos Reports Access*.

Optionally, use the *Explanation of Request* text box to enter comments about the access removal you are requesting for the applicant. If you are requesting removal of access for KFS inquiries and BI/Cognos GL reports, but not changing any account-specific access rights, you can submit the User Access Request eDoc without completing the rest of the **Remove Account Access (Inquiries, Payroll Expense Transfer, and Reports)** tab.

### Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)

The **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request that the applicant be authorized to view all account information belonging (a) to *individual* 10-digit Organization Codes, (b) to groups of Organization Codes that all start with the same 3-, 5-, or 7-digit “mask,” or (c) to *all* Organization Codes. You can also specify Account Numbers to be excluded from those to which the applicant will be granted access.

Note that this tab includes an **Import file** link that you can use to import multiple Organization Codes or masks at once when you are adding access rights. For instructions, see **Importing Multiple Lines of Data** on page 6.)

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

#### Instructions for Adding Access to Individual Organization Codes or to Organization Code Masks

1. In the uppermost section of the **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Organization Code* field as follows:
  - To request that the applicant be granted access to all accounts belonging to one specific Organization Code, enter the complete 10-digit Organization Code.
  - To request that the applicant be granted access to all accounts belonging to all Organization Codes that begin with the same digits, enter that 3-, 5-, or 7-digit “mask” followed by an asterisk (\*). Bear in mind that there are more Organization Codes associated with a 3-digit mask than with a 7-digit mask. Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 261\*).
  - To request that the applicant be given access to all accounts belonging to ALL Organization Codes, enter just an asterisk (\*).

If you entered an individual 10-digit Organization Code, the *Organization Code Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the Organization Code access changes you are requesting for the applicant.

**NOTE:** When requesting that the applicant be given access to the accounts belonging to an Organization Code, if there are specific account numbers that should be omitted from those to which he/she will have access, be sure to specify them as explained in the next section, **Instructions for Excluding Account Numbers When Adding Organization Code Access**.

### **Instructions for Excluding Account Numbers When Adding Organization Code Access**

Use the following procedure to specify any Account Numbers that should be excluded from the group of accounts belonging to an Organization Code for which the applicant will be granted access. The applicant will not be able to access the excluded accounts.

1. In the second section of the **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:
  - To request the exclusion of an individual account from an Organization Code, enter the complete 10-digit Account Number.
  - To request the exclusion of all accounts that begin with the same six numbers, enter that 6-digit mask followed by an asterisk (\*). Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 534854\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the Organization Code access changes you are requesting for the applicant.

### **Instructions for Adding Access to KFS Inquiries and Cognos Reports**

The *Inquiries and Reports: Choose Add Access* section of the **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request that the applicant be given access to run the General Ledger inquiries available on the KFS Financial Main Menu, and also (optionally) the BI/Cognos GL reports available on the Business Intelligence Portal for KFS.

**NOTE:** In order to run BI/Cognos GL reports, the applicant must also have access to run the KFS inquiries. When a user runs either inquiries or BI/Cognos reports, they will only contain data for those accounts to which he/she has been granted access rights at the Account or Organization Code level. If the applicant has been granted account-specific access for the Capital Assets Management System (discussed on page 24), then he/she will be able to view data for those same accounts in inquiries and BI/Cognos reports.

The *None* option is selected by default. To request that access be added, select another option:

- If you want the applicant to have access to run the KFS inquiries, but not the BI/Cognos GL reports, select the radio button labeled *Inquiries Access Only*.
- If you want to request that the applicant be granted access to run the KFS inquiries *and* the BI/Cognos GL reports, select the radio button labeled *Both Inquiries and Cognos Reports Access*.

Optionally, use the *Explanation of Request* text box to enter comments about the access changes you are requesting for the applicant. If requesting only access for KFS inquiries and BI/Cognos GL reports, and not the addition of any Organization Code–specific access rights, you can submit the User Access Request eDoc without completing the rest of the **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab.

### Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)

The **Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request removal of the applicant's access rights to view account information belonging (a) to *individual* 10-digit Organization Codes, (b) to groups of Organization Codes that all start with the same 3-, 5-, or 7-digit "mask," or (c) to *all* Organization Codes. You can also specify Organization Codes to be excluded from those for which the applicant will no longer have access rights.

Note that this tab includes an **Import file** link that you can use to import multiple Organization Codes or masks at once when you are deleting access rights. For instructions, see **Importing Multiple Lines of Data** on page 6.)

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

### Instructions for Removing Access to Individual Organization Codes or to Organization Code Masks

1. In the uppermost section of the **Add Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Organization Code* field as follows:
  - To request removal of the applicant's access to all accounts belonging to one specific Organization Code, enter the complete 10-digit Organization Code.
  - To request removal of the applicant's access to all accounts belonging to multiple Organization Codes that begin with the same digits, enter that 3-, 5-, or 7-digit "mask" followed by an asterisk (\*). Bear in mind that there are more Organization Codes associated with a 3-digit mask than with a 7-digit mask. Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 261\*).
  - To remove the applicant's access to all accounts belonging to ALL Organization Codes, enter just an asterisk (\*).

If you entered an individual 10-digit Organization Code, the *Organization Code Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the Organization Code access removal you are requesting for the applicant.

**NOTE:** When requesting removal of the applicant's access to the accounts associated with an organization code mask, if there are any account numbers to which he/she should still have access, be sure to specify them as explained in the next section, **Instructions for Excluding Account Numbers When Removing Organization Code Access**.

### Instructions for Excluding Account Numbers When Removing Organization Code Access

When requesting removal of the applicant's access to accounts belonging to an individual Organization Code or to an Organization Code mask, use this procedure if you want to specify any Account Numbers that should be excluded. The applicant will still be able to access the excluded accounts.

1. In the second section of the **Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab, complete the *Account Number* field as follows:

- To request the exclusion of an individual account from an Organization Code or from an Organization Code mask, enter the complete 10-digit Account Number.
- To request the exclusion of all accounts that begin with the same six numbers, enter that 6-digit mask followed by an asterisk (\*). Be sure to type the digits and the asterisk as an unbroken string with no spaces (example: 534854\*).

If you entered an individual 10-digit Account Number, the *Account Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

2. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
3. Optionally, use the *Explanation of Request* text box to enter instructions or comments about the Organization Code access removal you are requesting for the applicant.

### **Instructions for Removing Access to KFS Inquiries and Cognos Reports**

The *Inquiries and Reports: Choose Delete Access* section of the **Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab is used to request the removal of the applicant's access to run the General Ledger inquiries available on the Financial Main Menu in Kualii, and also the BI/Cognos GL reports available on the Business Intelligence Portal for KFS.

**NOTE:** In order to run BI/Cognos GL reports, the applicant must also have access to run the KFS inquiries. When a user runs either inquiries or BI/Cognos reports, they will only contain data for those accounts to which he/she has been granted access rights at the Account or Organization Code level. If the applicant has been granted account-specific access for the Capital Assets Management System (discussed on page 24), then he/she will be able to view information for those same accounts in inquiries and BI/Cognos reports.

The *None* option is selected by default. To request that access be removed, select another option:

- Select the radio button labeled *Cognos Reports Access Only* to request removal of the applicant's access to run the BI/Cognos GL reports, while leaving him/her the ability to run the KFS inquiries.
- To request removal of the applicant's access to run the KFS inquiries *and* the BI/Cognos GL reports, select the radio button labeled *Both Inquiries and Cognos Reports Access*.

Optionally, use the *Explanation of Request* text box to enter comments about the access removal you are requesting for the applicant. If you are requesting removal of access for KFS inquiries and BI/Cognos GL reports, but not changing any Organization Code-specific access rights, you can submit the User Access Request eDoc without completing the rest of the **Remove Organization Code Access (Inquiries, Payroll Expense Transfer, and Reports)** tab.

### **Payroll Business Intelligence Reporting Access**

The **Payroll Business Intelligence Reporting Access** tab is used to request changes to the applicant's access rights for running Business Intelligence (BI) reports that contain employee payroll data for accounts to which that user has access. If the applicant requires the ability to view reports containing payroll data at the Region Code (home department code) level, you can also request such access on this tab.



**NOTE:** Region Code security is not required to use payroll reporting; it is only needed by a select group of users. Most users merely need the access provided by their Account-level or Organization Code-level security settings, for which changes can be requested by completing the tabs immediately above the **Payroll Business Intelligence Reporting** tab (see page 31).


Complete this tab as follows to request the addition or deletion of the Payroll BI Reporting role, which permits the user to access the BI payroll data reports. This tab can also be completed for the sole purpose of requesting a change to the applicant's region code access.

1. If you are requesting the addition or deletion of the Payroll BI Reporting role for the applicant, select the appropriate option in the *Payroll BI Reporting Role* drop-down list. If the applicant already has the role and you merely want to request the addition or deletion of region code access, you do not have to select an option in the drop-down list as long as you complete the other sections of the **Payroll Business Intelligence Reporting Access** tab.
2. Select the appropriate check-boxes to indicate whether the applicant's ability to view payroll data reports will be (or already is) based on Account/Organization security, Region Code security, or both. Note that this is a required field. If you select the check-box for Region Code Security, the *Add or Delete Payroll Region Code Security* section will appear on this tab.

If you are merely requesting the deletion of the Payroll BI Reporting role for the applicant, you do not need to complete the rest of the *Add or Delete Payroll Region Code Security* section. If you are requesting the addition or deletion of region codes that will be used to restrict the applicant's ability to view payroll data, complete this section as follows:

- a. In the *Payroll Region Code Security* drop-down list, select the appropriate option to indicate whether you are requesting the addition or deletion of Region Code security.
- b. In the *Region Code* field, enter the region (home department) code for which access to payroll data reports should be added or deleted.
  - You may enter a region code "mask" by entering the first four or six digits of the region code, followed by the asterisk (\*) wildcard. If you enter a region code mask, note that it will include all region codes beginning with the specified numbers, so be sure that the mask includes only your own region codes.
  - If you enter a 10-digit region code, the *Region Code Name* field will automatically be populated with information corresponding to your entry when you press the TAB key or click elsewhere on the screen.

To search for a region code number, click the lookup icon  next to the *Region Code* field. The **Home Department Code Lookup** page will be displayed. In the *Department Code Description* field, enter the home department name, or enter part of the name with an asterisk (\*) wildcard representing any words or letters that precede or follow the letters you entered. Click the  button, and when the search results appear at the bottom of the lookup page, click the *Return Value* link for the desired home department. The User Access Request eDoc will be displayed again with the home department code you selected now entered in the *Region Code* field and the *Region Code Name* field populated automatically.

- c. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
  - d. Repeat these steps as needed to add other region codes for which you are requesting the addition or deletion of access to payroll data reports.
3. Use the *Explanation of Request* text box to enter comments about the payroll data report access changes you are requesting for the applicant.
  4. Make certain that the *Person Requests* section of the **Ad Hoc Recipients** tab is completed to route the eDoc to the applicant's SBO for approval. (Refer to **Submitting Your User Access Request eDoc** on page 7.) If an SBO is submitting the access request for himself/herself, there is still an approval required, but the SBO can either route the eDoc for self-approval or route it to his/her supervisor.

## BI Planning and Projections (P&P)

The **BI Planning and Projections** tab is used to add or remove user roles that enable the applicant to utilize projection model templates in the Business Intelligence Budget Planning and Projections tool, which uses budget data that is current as of 7:00 A.M. on each business day. The roles added by means of this tab provide access to the BI Planning and Projections templates, but the user's access to budget data is limited by other account-level and organization-level security restrictions within the Kualu and BI/Cognos systems. Budget projections are limited to the current fiscal year.

### Roles for the BI Planning and Projections templates:

- **Income & Expense Projection Department User** – This role will allow the applicant to access the Income and Expense (I&E) Department projection model.
- **Gifts and Endowments Projection User** – This role will allow the applicant to access the Gifts and Endowments (G&E) projection model.

The upper portion of this tab presents the basic instructions for adding or deleting BI Planning and Projections roles for the applicant:

1. Use the *Role Name* drop-down list to select the particular role to be added or removed for the applicant.
2. In the *Add/Delete Role* drop-down list, select the appropriate option to indicate whether you are adding or removing the role you specified in the *Role Name* drop-down list.
3. Click the  button in the *Actions* column. The line entry that you have just added to the eDoc will appear beneath the line on which you entered the information.
4. Repeat steps 1–3 as needed to add or delete other BI Planning and Projections roles for this applicant. Each role can be specified only once per eDoc, and an error message will be presented if you accidentally select the same role again.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.

## Other Requests

The **Other Requests** tab is provided so that you can enter instructions for user access changes that cannot easily be requested by completing any of the other tabs on the User Access Request form. To complete this tab, use the *Explanation of Other Requests* text box to enter instructions or a description of the access changes you are requesting for the applicant in question.

When you are ready to submit the User Access Request eDoc, proceed to **Submitting Your User Access Request eDoc** on page 7.



**INDEX**

- Account level access
  - adding, 31
    - BI/Cognos GL reports, 32 and 36
    - Capital Assets Management, 24
    - DV and DVQE, 21
    - individual accounts or masks, 31
    - Inquiries (KFS General Ledger), 32 and 36
  - removing, 33
    - BI/Cognos GL reports, 34 and 38
    - Capital Assets Management, 25
    - DV and DVQE, 22
    - individual accounts or masks, 33
    - Inquiries (KFS General Ledger), 34 and 38
- Ad Hoc Recipients tab (routing upon submittal), 7
- Advance Deposits; see *Cashiering*
- Applicant Information tab, 3
- applicant's current access information, 3
- attachments (optional), 5
- awards, financial aid; see *Financial Aid Account*
- BI Planning and Projections (P&P), adding or deleting user roles, 40
- Budget planning and projections, see *BI Planning and Projections (P&P)*
- Business Intelligence (BI/Cognos) reports
  - General Ledger reports
    - adding access, 32 and 36
    - removing access, 34 and 38
  - Payroll data reports
    - adding or removing access, 38
- Business Intelligence planning and projections, see *BI Planning and Projections (P&P)*
- Business Office Reviewer (adding or deleting account access for eStatements), 19
- CAMS; see *Capital Assets Management*
- Capital Assets Management, 24
  - adding access, 24
  - deleting access, 25
- Cash Receipts; see *Cashiering*
- Cashiering, 11
  - adding access, 11
  - deleting access, 11
- Chart of Accounts (changes and additions), 29
- Check requests; see *Disbursement Vouchers (DV/DVQE)*
- Cognos (Business Intelligence) reports
  - General Ledger reports
    - adding access, 32 and 36
    - removing access, 34 and 38
  - Payroll data reports
    - adding or removing access, 38
- copy an existing User Access Request eDoc to create a new one, 9
- Course Scheduling, 29
  - adding user to a workgroup, 29
  - deleting user from a workgroup, 30
  - requesting creation of a workgroup, 30
- creating a new eDoc by copying an existing one, 9
- Credit Card Receipts; see *Cashiering*
- Default Supervisor in Workday
  - for Disbursement Vouchers (DV/DVQE), 23
  - for eStatement, 18
- Department Organization Code (definition), 3
- Disbursement Vouchers (DV/DVQE), 20
  - adding access, 21
  - change supervisor, 23
  - default supervisor in Workday, 23
  - deleting access, 22
- Effort Certification (EC), adding or deleting roles, 17
- eMarket; see *Purchasing Accounts - Payable*
- equipment inventory; see *Capital Assets Management*
- eStatement, 18
  - Business Office Reviewer access, 19
  - change supervisor, 18
  - default supervisor in Workday, 18
  - proxy settings, 19
- excluding account numbers from account masks or Organization Codes
  - when adding access, 32 and 36
  - when removing access, 34 and 37
- Financial Aid Account (FAA), 27
- General Budget Change, adding or deleting roles, 24
- General Journal Vouchers; see *Journal Vouchers*
- General Ledger inquiries; see *Inquiries*
- General Purpose Workflow eDoc, 26
  - adding user to a workgroup, 27
  - deleting user from a workgroup, 27
  - requesting creation of a workgroup, 27
- GJVs; see *Journal Vouchers*

continued on following page...

- Import file (link), 6
- importing data, 6
- Inquiries (KFS General Ledger)
  - adding access, 32 and 36
  - removing access, 34 and 38
- Internal Billing, adding and deleting roles, 24
- Journal Vouchers (JVs), 20
  - adding access, 20
  - deleting access, 20
- JVs; see *Journal Vouchers*
- KFS Inquiries; see *Inquiries*
- Miscellaneous access changes; see *Other Requests tab*
- Module Selection tab, 4
- Notes and Attachments tab (optional), 5
- Organization Code level access
  - adding, 35
  - removing, 37
- Other Requests tab, 40
- Payroll data reports, access 38
- Payroll Expense Transfer (PET), add/delete roles, 17
- Planning and Projections (adding or deleting user roles for this Business Intelligence budget tool) 40
- P&P, see *Planning and Projections*
- Preparer Information tab, 3
- Procurement Card
  - eStatement, 18
    - Business Office Reviewer access, 19
    - change supervisor, 18
    - proxy settings, 19
  - Reallocation, 12
    - adding access, 12
    - deleting access, 13
- proxy settings (for eStatements), 19
- Purchasing - Accounts Payable (USC eMarket), 13
  - adding roles and permissions, 13
  - roles (descriptions), 14
  - removing roles and permissions, 15
- Quick Expense reimbursement requests; see *Disbursement Vouchers (DV/DVQE)*
- Region-level access to payroll data reports, 38
- reports, Business Intelligence (Cognos)
  - General Ledger reports
    - adding access, 32 and 36
    - removing access, 34 and 38
  - Payroll data reports
    - adding or removing access, 38
- roles
  - BI Planning and Projections, adding or deleting user roles, 40
  - Cashiering, add or delete roles, 11
  - DV and DVQE roles
    - adding access, 21
    - descriptions, 21
    - removing access, 22
  - Effort Certification, add or delete roles, 17
  - General Budget Change, add or delete roles, 24
  - Internal Billing, add or delete roles, 24
  - Payroll BI Reporting role, 39
  - Payroll Expense Transfer, add or delete roles, 17
  - SPA Budget Reallocation, add or delete roles, 26
  - USC eMarket roles
    - adding access, 13
    - descriptions, 14
    - removing access, 15
- Route Log (checking status after submittal), 8
- routing of an eDoc upon submittal, 7
- security; see *Account level access* and *Organization Code level access*
- SPA Budget Reallocation, add or delete roles, 26
- supervisor, changing
  - Disbursement Vouchers (DV/DVQE), 23
  - eStatement, 18
- USC eMarket; see *Purchasing Accounts - Payable*
- use an existing User Access Request eDoc to create a new one, 9
- user roles; see *roles*
- User Access Request eDoc
  - general information, 2
  - initiating, 2
  - saving before submittal, 8
  - submitting, 7
  - status after submitting, checking, 8
- View Applicant's Current Access tab, 3
- workgroups
  - Cashiering, 11
  - Course Scheduling, 29
  - General Purpose Workflow, 26