Access Control Executive

Procedures Manual & Reference Guide

DCATS
Information Management Client Support Services

Version XIII | May 2015
210-567-7777 Option 5
Table of Contents

INTRODUCTION ................................................................................................................................................. 3
ACE RESPONSIBILITIES AND DUTIES ............................................................................................................. 4
ACCESS CONTROL EXECUTIVE (ACE) DESIGNATION PROCEDURE ......................................................... 5
THE SCOPE OF ACE DUTIES ADMINISTRATIVE BUSINESS SYSTEMS AT HSC ........................................ 6
  ADMINISTRATIVE MAILBOXES ....................................................................................................................... 6
  DOCUMENT REVIEW SYSTEM ....................................................................................................................... 6
  DATA WAREHOUSE ..................................................................................................................................... 6
  EMPLOYEE SELF SERVICE ............................................................................................................................. 6
  eSHIPGLOBAL .............................................................................................................................................. 6
  FM SYSTEMS ................................................................................................................................................. 6
  HYPERION ...................................................................................................................................................... 6
  PORTAL .......................................................................................................................................................... 7
  PeopleSoft .................................................................................................................................................... 7
  PeopleSoft/HCM ......................................................................................................................................... 7
  PeopleSoft/Financials ................................................................................................................................. 7
  PeopleSoft/Student Administration ............................................................................................................ 7
ACCESS CONTROL PROCEDURES FOR UTHSCSA BUSINESS SYSTEMS .................................................... 8
  ACE Proxy .................................................................................................................................................. 8
  OBTAINING SECURITY ACCESS TO APPLICATION SYSTEMS .................................................................. 10
  DATA WAREHOUSE (DW) ............................................................................................................................ 10
  DOCUMENT REVIEW SYSTEM ................................................................................................................... 10
  PeopleSoft Financials Web Requisition ........................................................................................................ 11
  PeopleSoft Human Capital Management (HCM) ......................................................................................... 11
  PeopleSoft Student Administration ............................................................................................................ 12
  eSHIPGLOBAL ............................................................................................................................................ 12
  HYPERION ................................................................................................................................................... 13
  Blanket Travel Authorizations ..................................................................................................................... 14
TERMINATING SECURITY ACCESS TO APPLICATION SYSTEMS .................................................................. 15
SECURITY ACCESS PASSWORD PROCEDURE .............................................................................................. 15
PEOPLESOFT FINANCIALS REQUISITION SECURITY .................................................................................... 16
  TYPICAL ROLES .......................................................................................................................................... 16
  REVIEW DEPARTMENT SETUP ................................................................................................................... 17
REQUESTING AND SETTING UP A NEW OPERATOR ....................................................................................... 19
  ACTIVATING A PROFILE AND ASSIGNING ROLES .................................................................................... 19
UPDATING AN OPERATOR ............................................................................................................................. 22
REQUESTING AND SETTING UP A DW/HR PAY LISTING USER ................................................................. 24
P.O. DISPATCH ................................................................................................................................................. 26
REQUESTS STILL REQUIRING INTERVENTION FROM DCATS ..................................................................... 29
Introduction

Academic and Business Technology and Integrated Management Information Systems have custodial responsibility for the management of all HSC administrative business systems; however, departments maintain the responsibility for authorizing user access to systems for the completion of daily operations.

Fulfilling this responsibility, each UTHSCSA department must designate an Access Control Executive (ACE). The ACE must be appointed by the Dean, Chair, or Director through the Access Control Executive (ACE) Designation Form.

The ACE has the responsibility to manage departmental users accessing administrative business systems including: PeopleSoft applications, Document Review System (DRS), Data Warehouse (DW), Hyperion, and eShipGlobal. These systems contain sensitive data and information critical to HSC business processes. In addition to this critical function, the ACE serves as the official liaison between the departmental users, administrative departments, IMCSS and IMIS in the use of UTHSCSA administrative business systems.

Good internal control procedures provide the foundation for implementing secure administrative business systems. Therefore, it is required that the ACE be a senior member of the department: Dean, Chair, Director, Associate/Assistant Director, Administrator or the department's senior administrative position (provided the department's organization structure does not include an Associate/ Assistant Director or Administrator).

The ACE must be knowledgeable about the University policies and procedures, internal controls, and the department's business processes and organizational structure.

The Access Control Executive (ACE) Designation Form cannot be signed by anyone other than the Dean, Chair, or Director without approval from the Vice President and Chief Financial Officer.
ACE Responsibilities and Duties

Implementation of appropriate access controls to administrative business systems is critical to attainment of HSC’s missions. Deans, Chairs, and Directors, as well as the designated departmental ACE to ensure departmental compliance should carefully review the ACE responsibilities listed below. Failure to comply could put business processes and information at risk.

- The ACE has the responsibility to assign appropriate security access to all application systems. Departmental users should be assigned access privileges based on job duties, or on a “need-to-know” basis. Additionally, the ACE must ensure approval cycles support appropriate separation-of-duties and good internal controls.

- The ACE has the responsibility to immediately terminate security access for an employee who has been terminated, transferred to another department, or no longer has a need to access administrative systems.

- The ACE is required to review the “User Security Access Departmental List”, at least annually, and provide a signed copy to their Dean, Chair or Director. Any access changes should be forwarded to IMCSS for implementation. To document the completion of required ACE training and system access verification, the department must maintain a current signed copy of the list.

- In the ACE’s absence, only a designated ACE Proxy, or the Dean, Chair, or Director may assume the responsibilities and duties of the ACE.

- The ACE is required to attend mandatory annual training.

- The ACE has the responsibility to ensure departmental personnel receive both formal systems training and training related to departmental procedures and accounts.

- The ACE serves as the official liaison between the department, administrative departments, IMCSS and IMIS in the use of UTHSCSA's administrative business systems. Access control actions requested by the ACE will be implemented by the DCATS (Data Warehouse, Cactus Application Training and Support) team, a division of IMCSS.

- The ACE has the responsibility to maintain the electronic Administrative Mailbox, which is established for internal control of routine departmental business processes.

- The ACE has the responsibility to ensure personal computers accessing administrative business systems are properly secured.
Access Control Executive (ACE) Designation Procedure

1. To designate a departmental ACE, the Dean, Chair, or Director must scan and attach the completed and signed **Access Control Executive (ACE) Designation Form** upon submission of the request through the IMS Self Service Portal. The form must include the final signature from the VP & CFO, Andrea Marks.

2. The departmental ACE can also be the Technical Support Representative (TSR) and vice versa, the TSR can also be the departmental ACE.

3. To assign a new ACE, the department will need to complete the **ACE Designation form** and forward the signed form to the Vice President and Chief Financial Officer for approval.
   - It is the responsibility of the Vice President and Chief Financial Officer to grant or deny ACE nominations. The Vice President will then return the form to your office.
   - After signatures are complete, the current ACE will scan and attach the ACE Designation Form upon submission of your request through the IMS Self Service Portal.
   - DCATS will contact the newly appointed ACE to schedule initial ACE training. This training is required for NEWLY designated ACEs and is conducted one-on-one throughout the year.
   - This Initial ACE training includes a “technical” and “functional overview” and an initial review of Departmental Security Access and the appropriate forms.
   - An ACE Checklist is signed after the new ACE has completed one-on-one training stating the new ACE has reviewed the current application user lists.

4. Only the Vice President and Chief Financial Officer may sign the **Access Control Executive (ACE) Designation Form** in place of the Dean, Chair, or Director.

5. When a new ACE is designated, the name of the former ACE will be removed from distribution lists and all ACE security access will be terminated immediately.

6. As a review of responsibilities and existing departmental access, each ACE is required to attend annual ACE training.
   - Mandatory Annual ACE training is completed through online training and includes a “functional” overview and a review of departmental security access and the appropriate forms.
   - The ACE training includes the following documentation:
     - ACE Procedure manual
     - User Security Access Departmental List and Confirmation Form
     - Additional Process Guides as needed
   - After Annual Mandatory ACE training, original forms for the **User Security Access Departmental List Confirmation** and the **Mandatory Annual ACE Training Acknowledgement** are signed, scanned and attached by the ACE to the IMS Self Service portal request. A copy should be maintained by each department for records.

7. DCATS is responsible to maintain signed copies of the **ACE Designation Form** and the **User Security Access Departmental List Confirmation Form** within Supportworks, however we do not require departments to submit an original hardcopy to the DCATS office.
The Scope of ACE Duties

Administrative Business Systems at HSC

Administrative Mailboxes
UTHSCSA is utilizing a portion of the PeopleSoft enterprise system known as “workflow” to enhance the electronic document flow. Workflow generates an “FYI confirmation email” to support the business and approval processes for certain PeopleSoft transactions. These email messages are sent to the department’s administrative mailbox and must be maintained for documentation purposes. The departmental ACE functions as the owner of the mailbox and uses Microsoft Outlook for administration. Training on how to appropriately set up and use the administrative mailbox is provided during ACE training.

Document Review System
The Document Review System (DRS) is a web-based application that allows authorized users to submit and approve documents supporting certain business processes at the Health Science Center. At present, DRS provides access to time collection and leave accounting reports.

Data Warehouse
The Data Warehouse is a set of special databases containing institutional and departmental data. The Data Warehouse is accessed through a web-based software program and allows users to schedule and view pre-defined reports supporting daily operations and business decisions.

Employee Self Service
This PeopleSoft application allows employees to access and/or update personal information 24/7 from any computer with an internet connection. Also available for them is the ability to view all paychecks processed through payroll and their selected benefits.

eShipGlobal
This is the consolidated web-based shipping service used by UTHSCSA to process all letters and packages shipped via 3rd party carriers through Central Receiving. It is also available to departmental users for use within departments via the UTHSCSA portal. Departmental users can use this application software to schedule shipments, print air bills from their local printers and receive competitive pricing on shipments including negotiated State rates. eShipGlobal provides shipping services for Federal Express, UPS and DHL (Airborne Express).

FM Systems
The FM Systems has been created to assist with the annual space review process. This will allow the HSC departments to conduct their space allocation review online.

Hyperion
The Hyperion application allows employees to access and/or update Budget Planning information from any computer with an internet connection.
**Portal**
The portal serves as a gateway to a variety of resources and services, from organized content to applications, used at the Health Science Center.

**PeopleSoft**
PeopleSoft is the administrative software replacing major administrative business systems. This software will help achieve organizational goals by improving service levels.

**PeopleSoft/HCM**
The PeopleSoft HCM workflow process was implemented to assist users in navigating through the various panels needed to make any changes to an employee from the time of hire through termination.

**PeopleSoft/Financials**
The PeopleSoft Web Requisition is a web-based application that was developed to provide the University with a uniform purchase requisition and a uniform method of processing requisitions. This process is used to prepare a basic purchase requisition, a general stores requisition, a direct connect requisition or a travel requisition.

**PeopleSoft /Student Administration**
This product covers the areas of Admissions, Student Records, Financial Aid and Student Financials (tuition and fee billing and collection). Individuals make requests to Student Services for access to PeopleSoft Student Administration. In addition, the authorized point of contact who serves as liaison for the back office support, from the Registrar, Bursars and Financial Aid offices make requests for access. Student Services reviews the request, completes a User Security Access Request form and attaches the form upon submission of their request through the IMS Self Service Portal for DCATS to process.
Access Control Procedures for UTHSCSA Business Systems

For all access to the application systems, the departmental ACE is required to submit a Personnel Security Access Request (PSAR) form through the IMS Self Service Portal.

Please Note: For security reasons, the PSAR form can only be submitted by the departmental ACE. New and existing employees who are not in the ACE role, do not have access to this form and should not attempt to complete this form.

- The PSAR form is located in the UTHSCSA portal intranet system under the IMS Self Service Portal. [http://supportworks.win.uthscsa.edu/sw/selfservice/](http://supportworks.win.uthscsa.edu/sw/selfservice/)
- If the ACE is on vacation or out on leave, a proxy should be designated to submit an email to obtain emergency access for new/existing users to the UTHSCSA business applications via email, copying the Dean Chair or Director and Dept ACE.
- To set up an ACE proxy, the ACE must complete, scan and attach an ACE Proxy Designation form through the IMS Self Service Portal. DCATS will contact the ACE when completed.
- The ACE Proxy Designation form is located in the UTHSCSA portal intranet system under the IMS Self Service Portal.

This option in no way allows the proxy to take on the responsibilities of the ACE. This is for emergency situations only and should not be abused.

ACE Proxy

Due to the Access Control Executive’s (ACE) critical role to ensure the day-to-day operations of the department, it is imperative that the absence of the Access Control Executive (ACE) does not hinder or halt the department’s ability to operate. If the Access Control Executive (ACE) is out of the office and modifications need to be made to a departmental user’s access for any of the institutional administrative business systems, the Proxy has full authority to request the needed access by submitting an email to the DCATS Office. Once the DCATS Office receives the email request, a Service request will then be submitted to the appropriate back office personnel for completion.

Appropriate security measures should be followed for the institutional administrative business systems. The Proxy’s limited responsibilities are listed below and should be reviewed carefully by the ACE Proxy, Departmental ACE, and Dean, Chair, or Director.

In the ACE’s absence, the Proxy has the responsibility to request the appropriate security access to be granted, to the institutional business systems for their department personnel based on job duties, or a “need-to-know” basis.

ACE Proxy responsibilities should not be abused by the Departmental ACE. This method of action should only be used if the Departmental ACE is on vacation or using sick/personal leave.

- The Proxy must email DCATS with the request for access upon the ACE’s absence.
- The Proxy must copy their Departmental ACE and Departmental Dean, Chair or Director in the email to DCATS in the ACE’s absence.
- A confirmation Reply To All email will be sent from DCATS upon completion of the request.
The Proxy cannot request to delete access to any of the institutional administrative applications during the ACE’s absence.

The Proxy may be required to take ACE training.

The Proxy will agree to abide by the terms of all ACE Policies, including DCATS guidelines and the University’s Handbook of Operating Procedures.

The Proxy cannot access the ACE Tools or the PSAR form. It is against HOP Policy (5.8.4) for the ACE to share the domain username and password to allow Proxy’s to access these menu items.

Completing the PSAR form through the IMS Self Service Portal

Please note: This request MUST be completed by the departmental ACE.

Enter the following information:
- Employee ID and name of the employee for which access is requested.
- Department Name and ID
- Effective date for requested access change
- Department ID the employee will need access to

From the drop down arrow, select PSAR form and continue to review which software application you are requesting/deleting access for the user. Select N/A, Add, Delete or Transfer (if applicable).

The following listings are not an option to select unless you are in one of the departments:
- LAR – For Lab Animal Resources Employees Only
- Grants – For Office of Sponsored Programs Employees Only
- UT Police – For UT Police Employees Only

For DW access: If buying a new license, please submit a My Service request (see section on Obtaining Security access to DW). If transferring a current license to a user, submit the PSAR form and complete the DW section listing the employee id and name of the employee you are transferring the license from.
- If requesting the user have access to the HR Pay Listing report, be sure to check off the radio button in the Data Warehouse section of the PSAR form.

For DRS access:
- If requesting access for a new preparer, list the current approver’s name
- If requesting access for a new approver, list the current preparer’s name

The request will automatically be sent to the DCATS team for processing.

The ACE will receive a IMS Support Works confirmation email when the request is complete.
Obtaining Security Access to Application Systems

Data Warehouse (DW)

The Access Control Executive (ACE) submits a PSAR (Personnel Security Access Request) form to request security access to the Data Warehouse for a specific user. This user will be running reports and reconciling accounts for the department. If a new license needs to be purchased for a new user, the ACE should note that on the request. The My Services request must include the user’s name, employee ID number (EmplID), and department ID number (DeptID). A one-time charge of $250.00 per licensed user is billed to the requesting department if the ACE has requested a new DW license. The license may be transferred to another employee within the department at no charge, should the licensed user transfer or terminate.

1. The ACE submits the PSAR Form to the DCATS team for processing through the IMS Self Service portal. If transferring a Data Warehouse license, the ACE also submits a PSAR form through the IMS Self Service portal.
2. The DCATS team verifies the requested license and if applicable, bills the requesting department for the license. To ensure compliance with software privacy laws, a license is required for any user to use the Data Warehouse system.
3. Training is mandatory before access is granted. Once training is complete, a request is sent to the DW security team for set-up.
4. The DCATS team notifies the ACE when the access is complete via Supportworks Helpdesk email.
5. The user accesses Data Warehouse through the UTHSCSA Domain, which requires a domain username and password.
6. DCATS updates all necessary distribution lists and the User Security Access Departmental List. It is suggested the departmental ACE also update their departmental list as changes occur.

Document Review System

The Access Control Executive (ACE) submits a PSAR (Personnel Security Access Request) form to request security access to the Document Review System for a specific user. This user will be entering or approving Time Collection and/or Leave Accounting.

1. The ACE submits the PSAR Form to the DCATS team for processing through the IMS Self Service portal.
2. There is no mandatory training prior to access being granted for DRS by the App Security team. The new user is instructed to go to the DCATS website and print the DRS process guide for assistance. Ad-hoc classes or training via phone can be scheduled if requested.
3. The DCATS team notifies the ACE when the access is complete via Supportworks Helpdesk email.
4. DCATS updates all necessary distribution lists and the User Security Access Departmental List. It is suggested the departmental ACE also update their departmental list as changes occur.
**PeopleSoft Financials Web Requisition**

The Access Control Executive (ACE) will go to the Security page within PeopleSoft Financials, HSC Custom Components to authorize security access to the Financials Web Requisition system for a specific user. This user will be preparing online web requisitions.

1. Go to PeopleSoft Financials
   a. HSC Custom Components
   b. Security
   c. ACE Security
2. Enter a portion of the operator’s last name or complete last name and click the **Search** button.
3. The departmental ACE will add a Department ID within the User Access column and click the eShip checkbox if applicable.
4. Click the **SAVE** option.
5. There are no required classes to attend for Financials access before security access will be granted. However, it is recommended new users attend training.
6. DCATS updates all necessary distribution lists and the **User Security Access Departmental List**. *It is suggested the departmental ACE also update their departmental list as changes occur.*

**PeopleSoft Human Capital Management (HCM)**

The Access Control Executive (ACE) submits a PSAR (Personnel Security Access Request) form to request security access to the PeopleSoft HCM for a specific user. This user will be making changes in the HR area to include terminations, job maintenance and salary changes.

1. The ACE submits the **PSAR Form** to the DCATS team for processing through the IMS Self Service portal.
2. Training is mandatory before access is granted. Once training has been completed, an email is sent to the HCM Security team for set-up.
3. Security access is completed by the HCM Security team. The DCATS team notifies the ACE when the access is complete via Supportworks Helpdesk email
4. DCATS updates all necessary distribution lists and the **User Security Access Departmental List**. *It is suggested the departmental ACE also update their departmental list as changes occur.*
PeopleSoft Student Administration

The Access Control Executive (ACE) or assigned liaison, submits the User Security Access Request form to request security access to the PeopleSoft Student Administration for a specific user. This user will be accessing the Student Services menu options.

1. The assigned liaison(s) submits the **User Security Access Request form** to DCATS team for processing through the IMS Self Service portal. For Student Admin access, Lisa Serna, Mercedes Garcia and Ellen Nystrom are the responsible party for submitting these requests.

2. A hardcopy request form is scanned and attached to the request.

3. Security access is completed by the App Security team and then notification is sent to the assigned liaison(s) (Lisa Serna, Mercedes Garcia and Ellen Nystrom) via Supportworks Helpdesk email.

4. DCATS updates all necessary distribution lists and the **User Security Access Departmental List**. It is suggested the departmental ACE also update their departmental list as changes occur.

*Important note: For security reasons, the User Security Access Requests form can only be submitted through the authorized liaison for Student Admin access. New or existing employees who are not listed as a liaison, do not have access to this form and should not attempt to complete this form.*

EShipGlobal

The Access Control Executive (ACE) will go to the Security page within PeopleSoft Financials, HSC Custom Components to authorize security access to eShip Global system for a specific user. This user will be shipping items for their department.

1. Go to PeopleSoft Financials
   a. HSC Custom Components
   b. Security
   c. ACE Security

2. Enter a portion of the operator’s last name or complete last name and click the **Search** button.

3. The departmental ACE will add a Department ID within the User Access column and click the eShip checkbox.

4. Click the SAVE option.

5. There are no required classes to attend for eShipGlobal access before security access will be implemented. It is recommended the user review online training at the following link: [http://www.uthscsa.edu/business/avp/ESHIPGLOBAL/Training_Video.wmv](http://www.uthscsa.edu/business/avp/ESHIPGLOBAL/Training_Video.wmv)


7. DCATS updates all necessary distribution lists and the **User Security Access Departmental List**. It is suggested the departmental ACE also update their departmental list as changes occur.

8. For any questions related to shipping: contact Richard R. Gonzales at 210/567-5998 or gonzalesrr@uthscsa.edu
Hyperion

The Access Control Executive (ACE) submits a PSAR (Personnel Security Access Request) form to request security access to Hyperion for a specific user. This user will be making changes in the Hyperion Planning module to include entering Non-Salary numbers, Projection numbers, and also will project the budget for the next fiscal year.

1. The ACE submits the **PSAR Form** to the DCATS team for processing through the IMS Self Service portal.
2. The user should review all online tutorials prior to access being granted. In Knowledge Center, the user should review the following courses:
   a. Hyperion Budgeting
   b. Hyperion Reporting
   c. Position Budgeting in HCM
3. Security access is completed by the Hyperion Security team. The DCATS team notifies the ACE when the access is complete via Supportworks Helpdesk email.
4. If the user will be installing the Smart View application add-on, they must be pre-approved by the EC level. The user must then review the following courses:
   a. Introduction to Hyperion Smart View
   b. Gaining Smart view Aptitude
5. DCATS updates all necessary distribution lists and the **User Security Access Departmental List**. *It is suggested the departmental ACE also update their departmental list as changes occur.*
Blanket Travel Authorizations

To authorize individuals on Blanket Travel, the Access Control Executive (ACE) will go to Blanket Travel Authorizations within PeopleSoft Financials, HSC Custom Components. Updates made within the Blanket Travel Authorization page are reflected within the public inquiry, found within HSC Self Service Inquiry, Blanket Travel Inquiry.

A Travel Requisition is no longer needed for Blanket Travel since the Authorization is granted via the Blanket Travel Authorization page. Authorization is dependent on the home department for a user. Once the home department selects a user for Blanket Travel, the individual is authorized for any department.

1. Go to PeopleSoft Financials
   a. HSC Custom Components
   b. Blanket Travel Authorizations
   c. Add a New Value
   d. Enter the Business Unit, Department ID and Budget Period
   e. Click Add

   ![Blanket Travel Authorizations](image)

   1. Go to
   2. Department: T5700
   4. Add

2. Click the Select Employees button to choose the employee(s) who will be authorized for Blanket Travel reimbursements:

   ![Select Employees](image)

3. Click the Select All hyperlink or choose individual employees for authorization.
4. Click the Copy Selected Lines button
5. Click Save

The employees selected will now be listed within the HSC Self Service Inquiry – Blanket Travel Inquiry.
Terminating Security Access to Application Systems

The ACE has the responsibility to immediately terminate security access for an employee who has terminated, transferred from their department, or no longer has a need to access administrative business systems.

Termination of security access to PeopleSoft, DRS, and Data Warehouse is performed by the App Security team when the departmental ACE submits a PSAR Form through the IMS Self Service portal, at the time a user is terminated or transferred from their department.

The ACE should remove all the requisition authorization roles, dept id’s and project id’s found within the User Access Column, Department Approver and Project Approver columns in People Soft Financials for terminating employees.

To terminate a Principal Investigator (P.I.) from a grant project id, the ACE must first contact the Office of Sponsored Programs (OSP) and have Sponsored Programs delete the P.I.’s user name from the project id. The ACE can remove the user name from a Project ID in the ACE Tools only after the “old” P.I. name has been replaced with a “new” P.I. name through OSP.

Note: It is the responsibility of the departmental ACE to confirm emails of a terminated employee. You have 10 days to send a service request form to IMCSS to retain the listed accounts if it is incorrect. Do not ignore these emails.

Security Access Password Procedure

Access to the Portal is controlled by the user’s domain login password for the UTHSCSA domain. This password expires every 60 days and must be reset by the user or contact the IMS Service Helpdesk at (210) 567-7777 option 1, to request the user’s domain password to be reset. The user can also visit the IMS Service desk office with a UTHSCSA ID badge.

Access to the Document Review System (DRS), Data Warehouse (DW) and Hyperion is controlled by the user’s domain login password for the UTHSCSA domain. This password expires every 60 days and must be reset by the user or contact the IMS Service Helpdesk at (210) 567-7777 option 2, to request the user’s domain password be reset. The user can also visit the IMS Service desk on the 4th floor of the Medical School building with their UTHSCSA ID badge available.

Manual reset by the user could be obtained by accessing “P-Sync,” the online Password Resetting utility tool. After successfully answering a personal questionnaire, the user will have the ability to pick a new password.
PeopleSoft Financials Requisition Security

The ACE has the responsibility to set up and maintain requisition authorizations for the PeopleSoft Financials web-client for front-office users. The intent is to provide details about the unique setup for UTHSCSA for Project and Department Approvers, and the ability for the ACE to make updates, directly for, the majority of their requisition authorization requests.

The major processes reviewed are:

- Review typical roles
- Requesting and setting up a new operator
- Maintaining operator authorization
- Review Requisition Authorization setup by department

Typical Roles

The chart below depicts the 3 roles (Requestor, Department Approver and Project Approver) that are common amongst financial front-office users.

- A **Requestor** (Preparer) has the capability to enter requisitions in the system. A requestor is designated at the department level.
- A **Department Approver** is the equivalent to a reviewer role. The Department Approver is associated with a department id.
- A **Project Approver** is the equivalent of the authorized signature approval. It is associated with a particular project ID.
Review Department Setup

In order to assist the ACE in maintaining their Requisition Authorization information, the Department Inquiry page will allow the ACE to review the current setup for an entire department. The Department Inquiry panel can be accessed via the Portal in the ACE Tools folder.

Select the department for review by entering the department id or searching for the department.

- Go to PeopleSoft Financials
  - a) HSC Custom Components
  - b) Security
  - c) Department Inquiry
- To search for the department, enter a portion of the department id or department description and click the **Search** button.
- Click on your department id to view a listing of access for your department.
Once displayed, the Department Inquiry will show the ACE all the Requestors, Department Approver, and Project Approver for that department. The Project Approver column indicates online approval authority as well as paper approval.

By clicking next to the Project Approver's name, a display will contain all the project ids for that Project Manager within that department. The “Signature Inquiry by Project Approver” within the Self Service Inquiries link can be used to find all the project ids for a Project Approver regardless of department. Additionally, the list of projects shows the current project status of “Active” or “Inactive”. The ACE might want to remove inactive projects from the Project Approver’s setup if they are no longer available to purchase against.
Requesting and Setting up a new operator

Activating a Profile and Assigning Roles

To begin the setup of a new PeopleSoft Financials web requisition user, the departmental ACE must first locate the individual within the ACE Security page. Specific operator roles, which are predefined, provide the user access to certain menu roles within PeopleSoft Financials. The ACE will need to unlock the individual’s account, activate the individual and assign user roles, to include deptid’s and projectid’s, needed for the user to perform their job duties.

Locate the operator in the Security page by entering a portion of the operator’s last name or the complete last name, and click the **Search** button.

- Go to PeopleSoft Financials
  - a) HSC Custom Components
  - b) Security
  - c) ACE Security
- Enter a portion of the operator’s last name or complete last name and click the **Search** button.
- Select the appropriate operator id by clicking on the name to bring up the operator’s requisition security information.

ACE Security
Enter any information you have and click Search. Leave fields blank for a list of all values.

<table>
<thead>
<tr>
<th>User ID: begins with</th>
<th>Name: begins with</th>
<th>Case Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>WONG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Search Results
View All  First 1-4  of 4  Last
<table>
<thead>
<tr>
<th>User ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WONGK</td>
<td>Wong Kim - term</td>
</tr>
<tr>
<td>WONGLM</td>
<td>Wong Leslie M</td>
</tr>
<tr>
<td>WONGRO</td>
<td>Ortiz-Wong Rachel</td>
</tr>
<tr>
<td>WONGSC</td>
<td>Wong Stanley C</td>
</tr>
</tbody>
</table>

A person who does not currently have a PeopleSoft Financials operator profile will have the **Account Locked Out** option selected by default. The ACE will also need to click the **Add Operator** button for a new PeopleSoft Financials user.
1. Unlock Account
2. Add Operator
3. Click SAVE

The security columns for the user should now be accessible. The ACE can assign access as needed for job duties.

- Left column indicates which dept id’s this operator can prepare requisitions for.
- Center column indicates which deptid the operator can approve for as Department Approver.
- Right column indicates which project id the operator can approve for as Project Approver.
Once the user is setup, the role (Requestor, Department Approver, or Project Approver) information will be available for input.

When searching for a user who already has a PeopleSoft Financials profile, you will select their name and add access as needed for job duties.

**Maintaining Operators**

The ACE will use the ACE Security panel to input a user’s requisition authorization preferences. This process includes the following functions:

- Adding, changing or deleting a Requestor department id
- Adding, changing or deleting a Department Approver department id
- Adding, changing or deleting a Project Approver project id.
Updating an Operator

Each ACE is assigned control over a single or group of departments within the PeopleSoft system. The ACE will only be able to add, change and delete information for the departments under his/her authority. A PSAR request from the ACE should be sent to the DCATS team through the IMS Self Service Portal to have a department added or deleted from an ACE’s security record.

Multiple ACEs can maintain a single Requestor’s profile if the operator has requestor and/or approver functions across different departments. This restriction will prevent unauthorized or accidental modification that could negatively affect all project ids for that Project Approver.

- Go to PeopleSoft Financials
  - a) HSC Custom Components
  - b) Security
  - c) ACE Security

- Locate the operator in the ACE Security panel by entering a portion of the operator’s last name, or complete last name, and click the **Search** button.

- Select the appropriate operator id by clicking on the name to bring up the operator’s requisition security information. The save button will be activated if you make any changes to the operator.

- To save your updates, click the **Save** button.

- **Email ID:** The email address is used to route information between operators during the requisition approval process. If an ACE observes the email address is missing, send an email to DCATS at **dcats@uthscsa.edu** for assistance.

- Inserting additional departments or project ids in the panel can be accomplished by clicking the Add a new row button, type in the Department Id and click the **Save** button.

- Deleting departments or project ids in the panel can be accomplished by clicking the delete a row button, then click the **Save** button.

- For transfers to another department or termination requests, the ACE should remove all department id’s they are owner of prior to submitting the termination PSAR form.
Requestor/Preparer – User Access Column

- **Department ID:** The ACE will type in the department id or list of department id’s the operator will need access to view or to prepare requisitions for. The magnify glass can be used to display the entire list of valid departments within the PeopleSoft Financials system.

- **Inquire Only:** Check this flag when the operator needs to view requisitions for this department, but not to create/update them. All Department Approvers and on-line Project Approvers need “Inquiry” access to view requisitions within the departments when they approve. Once checked, the department is grayed out to reinforce the designation of inquire only access. You must uncheck the box to make modifications or delete the row.
  - The box MUST be unchecked under “inquiry only” to enable the operator to create requisitions for that department. If a Requestor is also an Approver, leaving the box unchecked provides the approver with requisition inquire and update access.

- **eShip:** Check this flag if the individual will be accessing the eShip Global page.

- **PBI Access:** Check this flag when the operator needs to view key balances for a project ID without having to access the Data Warehouse. Be reminded: the operator will be able to view all free balances for all project id’s which fall under a dept id they received PBI access to.
  - PBI Inquiry is listed within the Self Service Inquiries.

Department Approver

- **Department ID:** The ACE will type in the department id or list of department id’s the operator will need access to view as Department Approver or to prepare requisitions for. The magnify glass can be used to display the entire list of valid departments within the PeopleSoft Financials system.
  - Note - When you add a department id to the Department Approver column and that department does not exist in the User Access Column, the system will automatically add the department id to the User Access Column as Inquiry Only. This will allow the approver to view the requisition before approving it.

- The Department Approver approves travel requisitions for Foreign travel, then all Foreign travel requisitions will automatically be forwarded to the VP and CFO when both approver roles have approved the requisition.

- The Department Approver approves hazardous/radioactive requisitions, then all Environmental Health and Safety requisitions will automatically be forwarded to Environmental Health and Safety when both approver roles have approved the requisition.
Project Approver

- **Project ID**: The ACE will type in the department id or list of departments id’s the operator will need access to view as Project Approver or to prepare requisitions for. The magnify glass can be used to display the entire list of valid project ids within the PeopleSoft Financials system.
  - Note - When you add a project id to the Project Approver column and that department does not exist in the User Access Column, the system will automatically add the department id to the User Access Column as Inquiry Only. This will allow the approver to view the requisition before approving it.

- **On-line & Manual (paper-only)**: The on-line Project Approver can approve requisitions through the PeopleSoft Financials (Web Req) system and also has manual signature authority outside of the PeopleSoft system.
  - The designation of on-line or manual is all-inclusive for every project id listed for this Project Approver.

Requesting and Setting up a DW/HR Pay Listing User

To begin the setup of a DW user needing to view the HR Pay Listing report, the departmental ACE will need to submit the PSAR request to the DCATS team for processing through the IMS Self Service Portal, if not a current DW user, or if the user already has access to DW. DCATS will add the HR Pay Listing security access role.

- Complete the PSAR form by checking off the HR Pay Data radio button, then click on Submit.
- **Note**: In order to have access to HR Pay Data reports, the user will need a DW License.
After receiving a confirmation email via Supportworks Helpdesk from DCATS, the ACE will need to complete the following steps.

- Go to the Portal Menu
  - a) ACE Tools
  - b) Data Warehouse Security
- Enter the operator’s domain username or a portion of the operator’s last name and click the Search button.

Select the correct operator whose profile needs adjustments.

**Data Warehouse Security**

Enter any information you have and click Search. Leave fields blank for a list of all values.

- Find an Existing Value
- Search by: User ID begins with
  - Case Sensitive
  - Search | Advanced Search

**Search Results**

<table>
<thead>
<tr>
<th>User ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUTEAN</td>
<td>Cutean, Beverly J</td>
</tr>
<tr>
<td>CUTSHALL</td>
<td>Cutshall, Debra J</td>
</tr>
</tbody>
</table>
To add access to an operator’s profile, click the plus sign + to add a new department or the minus sign - to remove a department.

Select the HR checkbox for each department id added for the user. This option must be selected to complete the permissions for access. If this checkbox remains unchecked, the operator will be unable to view and run the HR Pay Listing Report.

Click “Save” button in the bottom left corner to make changes effective.

**Note:** Adding Data Warehouse departmental access for a specific user in Data Warehouse Security **DOES NOT** automatically grant access to the Data Warehouse system, nor does it imply the user has a license to use the Data Warehouse.

This function assumes the user already has current access to the Data Warehouse and only grants the user access to run the HR Pay Data report.

---

**P.O. Dispatch**

The PO Dispatch Notification Process will accelerate and expand communication of purchase order issuances. The PO Dispatch Notification Process will automatically send e-mail to departmental requesters and requisition contacts to notify them when a purchase order has been issued for their requisition.
Below is an example of the email notification sent to the requester, contact person and any additional persons listed.

```
From: PeopleSoft[psh@akasha.uthscsa.edu]  To: DOE@UTHSCSA.EDU, SMITH21@UTHSCSA.EDU  
Cc:  
Subject: Proj 16310/Fund 14001 PO 0000431534 COMPUTER EXPRESS (REQ 0000042707 COMPUTER EXPRESS) - Message (Plain Text)  

This notification is automatically generated. Please do not respond to this email, as it will not be monitored.  

---------------------------------  
Your requisition 0000042707 has been sourced to purchase order 0000431534. The PO was issued to  
COMPUTER EXPRESS on or before 11/19/2006. Prior to receipt of the PO items, please  
direct any inquiries about this PO to the buyer assigned to the purchase order, Pauline Sardinsky, who may be contacted by email at PurchAdmin@uthscsa.edu, or by phone at (210) 367-5030.  

You can view and/or print the purchase order in the HSC Portal at http://inside.uthscsa.edu/  
```

Besides the requester and requisition contact person, it may be desirable for others in the department to be notified of purchase order issuances. The departmental ACE will have the option of designating up to six additional persons to receive notifications whenever a purchase order is issued for one of the department’s requisitions.

- Go to PeopleSoft Financials
  - HSC Custom Components
  - Security
- PO Dispatch Notifications
Enter the deptid or the first letter of the deptid and click the **Search** button.

Add the correct e-mail address of any person(s) who should receive the PO notifications.

Click **SAVE**

Each time a PO is issued for one of the department’s requisitions, the person(s) designated on the PO Dispatch panel will receive an e-mail identical to the e-mail sent to the departmental requester and requisition contact.
Requests still requiring intervention from DCATS

The departmental ACE is still required to send an email request to the DCATS team for the following issues:

- Mass updates, personnel moves, or similar changes can be accomplished through the new Requisition Security panel. However, the time involved to make these changes online might warrant the ACE to submit the request to the DCATS team so the mass updates and/or move can be made programmatically.

The departmental ACE is still required to submit a PSAR request to the DCATS team for processing through the IMS Self Service Portal to the DCATS team for the following issues:

- Requests to add Preparers, Department Approvers and Project Approvers for department Z9001, or the projects associated with Z9001. The ACE will use the Comment Box and type the following information:
  - Example: Please add Z9001 to current Financials access for (Empl Name) as Project Approver
  - Example: Please add Z9001 to current Financials access for (Empl Name) as Department Approver
  - Example: Please add Z9001 to current Data Warehouse access for (Empl Name)

- Requests for access for POI’s
  They do not automatically have a profile created for them due to them not being actual employees at UTHSCA.