# Table of Contents

INTRODUCTION .................................................................................................................. 4  
WHAT IS AN ACE? ............................................................................................................... 4  
ACE RESPONSIBILITIES AND DUTIES ............................................................................ 5  
ACCESS CONTROL EXECUTIVE (ACE) DESIGNATION PROCEDURE ...................... 6  
ACE PROXY ........................................................................................................................ 7  
SECURITY ACCESS PASSWORD PROCEDURE ............................................................ 8  
THE SCOPE OF ACE DUTIES ADMINISTRATIVE BUSINESS SYSTEMS AT HSC ........ 8  
ADMINISTRATIVE MAILBOXES ....................................................................................... 8  
DOCUMENT REVIEW SYSTEM ......................................................................................... 8  
DATA WAREHOUSE ........................................................................................................... 8  
EMPLOYEE SELF SERVICE ............................................................................................... 8  
eSHIPGLOBAL ..................................................................................................................... 8  
FACILITIES MANAGEMENT SYSTEMS ............................................................................. 9  
HYPERION ......................................................................................................................... 9  
PAYMENT REQUEST ......................................................................................................... 9  
PORTAL ............................................................................................................................... 9  
PEOPLESoft ....................................................................................................................... 9  
PEOPLESoft/HUMAN CAPITAL MANAGEMENT ......................................................... 9  
PEOPLESoft/Financials ..................................................................................................... 9  
PEOPLEsoft /STUDENT ADMINISTRATION .................................................................. 9  
ACCESS CONTROL PROCEDURES FOR UTHSCSA BUSINESS SYSTEMS ............. 10  
Completing The Personnel Security Access Request (PSAR) Form Using The IMS Self Service Portal .......................................................................................................................................................................................... 10  
REQUESTING/GRANTING SECURITY ACCESS TO APPLICATION SYSTEMS ............. 12  
Blanket Travel Authorizations ......................................................................................... 12  
DATA WAREHOUSE (DW) ................................................................................................ 13  
DOCUMENT REVIEW SYSTEM (DRS) ............................................................................ 14  
eSHIPGLOBAL..................................................................................................................... 14  
HYPERION ......................................................................................................................... 15  
PAYMENT REQUEST ......................................................................................................... 16  
PEOPLESoft Human Capital Management (HCM) ........................................................... 16  
PEOPLEsoft Student Administration ............................................................................... 16  
PEOPLEsoft Web Financials Web Requisition ................................................................. 17  
TERMINATING SECURITY ACCESS TO APPLICATION SYSTEMS ............................ 17  
PEOPLESoft Financials Requisition Security ................................................................ 18  
REVIEW DEPARTMENT ID SECURITY ............................................................................ 19  
USER ACCESS TAB ........................................................................................................... 19  
DEPARTMENT APPROVER ACCESS TAB ...................................................................... 20  
PROJECT APPROVER ACCESS TAB ............................................................................... 21  
REQUESTING AND SETTING UP A NEW OPERATOR .................................................... 23  
NAVIGATION ..................................................................................................................... 23  
SECTION INFORMATION ............................................................................................... 24  
SECTION 1 – THE HEADER TABS .................................................................................... 24  
SECTION 2 – THE ACTION BOX ..................................................................................... 25  
SECTION 3 – THE FILTER AND SEARCH CRITERIA BOX ............................................ 26  
SECTION 4 – THE ACCESS DATA BOX .......................................................................... 27  
The User Access View within the Access Data Box ......................................................... 27  
The Department Approvers view within the Access Data Box ....................................... 28  
The Project Approvers view within the Access Data Box .............................................. 29  
UPDATING AN OPERATOR PROFILE/ADDING ACCESS ............................................. 30  
PREPARE ACCESS ........................................................................................................... 30  
DEPARTMENT APPROVERS ACCESS .......................................................................... 30  
PROJECT APPROVERS ACCESS .................................................................................... 31
Introduction

IMS – Business Support Services 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.

What is an ACE?

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, and IMS 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.

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 in the next page.

Failure to comply could put business processes and information at risk.
ACE Responsibilities and Duties

The departmental ACE has the following responsibilities and duties:

- 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 IMS 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, and Information Management Services in the use of UTHSCSA’s administrative business systems. Access control actions requested by the ACE will be implemented by the Application Security team or the Transition Solutions team (formerly known as DCATS), a division of IMS.

- 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

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.

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

1. 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 the departmental office.
   - After signatures are complete, the current ACE will scan and attach the ACE Designation Form to a service request on the IMS Self Service Portal.
   - The newly appointed ACE will be contacted 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,” a review of current Departmental Security Access, and overview of 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.

2. 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.

3. 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.

4. As a review of responsibilities and existing departmental access, each ACE is required to process ACE Annual Access Review documentation.
   - Mandatory Annual ACE training may be required and is completed through online training. This includes a “functional” overview, a review of current departmental security access, and overview of the appropriate forms.
   - The ACE training includes the following documentation:
     - ACE Procedure manual
     - Departmental User Security Access Confirmation List
     - Additional Process Guides as needed
   - Upon completion of the Mandatory Annual ACE review, the original forms for the Departmental User Security Access Confirmation List and the Mandatory Annual ACE Training Acknowledgement are to be signed, scanned, and attached by the ACE to an IMS Self Service portal request. Each department should maintain the original copies for their records.

5. Application Security is responsible to maintain signed & scanned copies of the ACE Designation Form and the Departmental User Security Access Confirmation List with the Security Access application. Departments are not required to submit an original hardcopy to the Application Security office.
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 are necessary for 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 Transition Solutions office at DCATS@UTHSCSA.EDU. Once the Transition Solutions office receives the email request, a Service Request will 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 the department personnel based on job duties, or a “need-to-know” basis.

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

- The Proxy must email Transition Solutions with the request for access upon the ACE’s absence.
- The Proxy must copy the Departmental ACE and Departmental Dean, Chair or Director in the email to Transition Solutions in the ACE’s absence.
- A confirmation Reply To All email will be sent from Transition Solutions 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 Transition solutions 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 a Proxy to access these menu items.
Security Access Password Procedure

Access to the Inside UTHSCSA Portal as well as the Document Review System (DRS), Data Warehouse (DW) and Hyperion applications are 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 online or by contacting the IMS Service Helpdesk at (210) 567-7777 option 1, to request the user’s domain password to be reset. The user may also visit the IMS Service Desk walk-in locations on the San Antonio campus with a UTHSCSA ID badge.

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 by the Transition Solutions team 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 entered supporting hours worked for part-time employees or overtime hours for salaried employees, as well as vacation and sick hours for employees and staff 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
Employee Self Service is a PeopleSoft application that allows employees to access and/or update personal information 24/7 from any computer with an internet connection. Employees may also view all paychecks processed through the UTHSCSA payroll as well as selected benefits.

eShipGlobal
eShip Global 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 inside.UTHSCSA.edu portal. Departmental users may use this application software to schedule shipments, print air bills from a local printer and receive competitive pricing on shipments including negotiated State rates. *eShipGlobal* provides shipping services for Federal Express, UPS and DHL (Airborne Express).
Facilities Management Systems
The FM Systems is designed to assist with the annual space review process. This system allows 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.

Payment Request
The Payment Request is an automated LV/SV processing system. It is designed to allow users to electronically generate, submit for processing/approval and track status of service and reimbursement voucher requests. This process is not for travel or purchase order payments.

Portal
The inside.UTHSCSA.edu 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 a collection of software for administrative business systems.

PeopleSoft/Human Capital Management
The PeopleSoft HCM workflow process was implemented to assist users navigate through the various panels needed to make any changes to an employee record from the time of hire through termination.

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

PeopleSoft /Student Administration
The Student Admin application 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, including the Registrar, Bursars and Financial Aid offices to make requests for access. Student Services reviews the request, completes a User Security Access Request form and attaches the form upon submission of a request through the IMS Self Service Portal for processing.
Access Control Procedures for UTHSCSA Business Systems

For 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, only the departmental ACE can submit the PSAR form. 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.
- The ACE Proxy Designation form is located in the UTHSCSA portal intranet system under the ACE Webpage at: [http://ims.uthscsa.edu/technology_support/dcats_ACE.aspx](http://ims.uthscsa.edu/technology_support/dcats_ACE.aspx)

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.

Completing the Personnel Security Access Request (PSAR) form using the IMS Self Service Portal

**This request MUST be completed by the departmental ACE**

The ACE logs into the IMS Self Service app with the domain ID and password, using the following link: [http://supportworks.uthscsa.edu/sw/selfservice/](http://supportworks.uthscsa.edu/sw/selfservice/)

1. Click on My Services
2. Click on the plus (+) sign in front of the Accounts and Access Management section
3. For the Business Application Access section, click the Raise Request button
4. Type in the Employee ID for the user needing access
5. Type the Employee Name for the user needing access
6. Type the Department Name
7. Type the Dept ID
8. Type the Effective date for requested access change
9. Enter the Department ID(s) the employee will need access to. The ACE can only request access to the DeptID(s) they are owner of.
10. From the drop down arrow, select PSAR form

Select type of HSC Business Application Access

- Select Choice-
  - ACE/ACE Proxy
  - PeopleSoft Student Administration
  - PSAR
  - RAHC Portal
  - UT Police
The following listings are not an option to select unless the ACE is in one of these departments:

- RAHC – For RAHC employees/student in the valley
- UT Police – For UT Police Employees

The form will guide the ACE through all Business Applications. Select N/A, Add, Delete or Transfer (if applicable) for all that applies. An option must be selected for every business application. If access for an application is not requested, select N/A, the section cannot be left blank.

Continue to click on Next until the request has been completed. Click the Submit button and receive a system generated request number. At this point, the ACE will also have the option to attach a file, or document to the request.

The request will automatically be submitted for processing.

The ACE will receive an IMS Support Works confirmation email when the request is complete.
Requesting/Granting Security Access to Application Systems

Blanket Travel Authorizations

University policy requires all departments to complete a PeopleSoft travel requisition for faculty, staff, interns, students and residents for all travel on University time or business away from the individual’s headquarters city when such travel will occur during an employee’s normal working hours.

To authorize individuals on Blanket Travel, the Access Control Executive (ACE) will go to Blanket Travel Authorizations within PeopleSoft Financials. 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 not needed for Blanket Travel since 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. Only the departmental ACE has update authority.

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

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

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 appear on the HSC Self Service Inquiry – Blanket Travel Inquiry. This authorization will be effective for the entire fiscal year. The departmental ACE must add users to Blanket Travel Authorization every fiscal year.
Once the page is saved, rows cannot be deleted. For employees no longer employed by the department or for whom a blanket authorization is no longer required, the ACE can change the status for the employee’s blanket authorization to Inactive.

**Transfer Employees**

If an employee transfers to another department, the departmental ACE where the employee transferred INTO must add the employee to the new departments’ blanket travel authorization list. The employee will not automatically be removed from the departments’ list they transferred OUT of. If the losing department wants to remove the employee’s name from displaying in the department listing, the ACE can change the status to “Inactive”. The department the employee transferred out of will still see the employee ID from the listing; however, the name will not show.

Click Save after making any changes to the current view.

**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 notate that on the request. 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 for processing through the IMS Self Service portal.
   - If transferring a current license to another user, list the employee ID and name of the employee the license is being transferred FROM.
   - If requesting the user have access to the HR Pay Listing report, the radio button in the Data Warehouse section of the PSAR form should be checked.
2. The Transition Solutions team verifies the requested license and if applicable, bills the requesting department for the license. If transferring a Data Warehouse license, the ACE should notate the employee ID being removed in the DW license FROM. To ensure compliance with software privacy laws, a license is required for every user who runs reports in the Data Warehouse system.
3. DW Training is mandatory before access is granted. Once training is complete, a request will be sent to the IMS Application Security team for processing.

4. The ACE is notified via Supportworks email when the access is complete. All necessary distribution lists and the Department User Security Access Confirmation Lists are updated. It is suggested the departmental ACE also update the departmental list as changes occur.

**Document Review System (DRS)**

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 for processing through the IMS Self Service portal.
   1. If requesting access for a new preparer, list the current approver’s name
   2. If requesting access for a new approver, list the current preparer’s name
2. There is no mandatory training prior to access being granted for the DRS application by the IMS Application Security team. The new user is instructed to view the Transition Solutions (DCATS) website and view the DRS process guide for assistance. Ad-hoc classes or training via phone may be scheduled if necessary. Contact Transition Solutions to schedule a training session.
3. The ACE is notified via Supportworks email when the access request is complete. All necessary distribution lists and the Department User Security Access Confirmation Lists are updated. It is suggested the departmental ACE also update the departmental list as changes occur.

**eShipGlobal**

The Access Control Executive (ACE) will go to the Security page within PeopleSoft Financials to authorize security access to eShip Global system for a specific user. This user will ship items for the department.

1. Go to HSC Business Applications
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 tab and click in the eShip Global 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)

For any questions related to shipping contact Jarrod Fischer at 210/567-5998 or fischerjt@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 projecting the budget for the next fiscal year.

1. Before the ACE submits a PSAR form for Hyperion access, they must first obtain approval from their EC office to add/delete Hyperion access for a user. This email showing EC approval, should be attached to the IMS Self Service request submitted when the ACE requests Hyperion access for a user.
2. The ACE submits the PSAR form for processing through the IMS Self Service portal. The EC approval email must be attached before Hyperion access is processed.
3. 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
4. If the user will be installing the Smart View application add-on, they must be pre-approved by the Budget office and the EC level. The user must then review the following courses:
   a. Introduction to Hyperion Smart View
   b. Gaining Smart View Aptitude
5. The ACE is notified via Supportworks email when the access is complete. All necessary distribution lists and the Departmental User Security Access Confirmation lists are updated. It is suggested the departmental ACE also update the departmental list as changes occur.
Payment Request

The Access Control Executive (ACE) will add Payment Request access at their discretion and on a “need to know” basis for the user. This user will be preparing or approving online payment requests.

1. The ACE logs into the UTHSCSA Portal
   a. HSC Business Applications
   b. ACE Tools
   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 should refer to “Requesting and Setting up a New Operator” for detailed steps on adding payment request user access.
4. Click the SAVE option.
5. The ACE should instruct the user to complete online training before the user attempts to prepare or approve payment requests.
   All necessary distribution lists and the Departmental User Security Access Confirmation Lists are updated. *It is suggested the departmental ACE also update the 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 for processing through the IMS Self Service portal.
2. Mandatory training must be completed before access is granted. Once training has been completed, an email is sent to the IMS Application Security team for processing.
3. The ACE is notified via Supportworks email when the access is complete.
   All necessary distribution lists and the Departmental User Security Access Confirmation Lists are updated. *It is suggested the departmental ACE also update the 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 request through the IMS Self Service portal. For Student Admin access, Lisa Serna, Mercedes Garcia and Ellen Nystrom are authorized to submit these requests.
2. A User Security Access Request form (hardcopy request form), is scanned and attached to the request.
3. Security access is completed by the IMS Application Security team and then notification is sent to the assigned liaison(s) (Lisa Serna, Mercedes Garcia and Ellen Nystrom) via Supportworks email.
All necessary distribution lists and the Departmental User Security Access Confirmation Lists are updated. It is suggested the departmental ACE also update the departmental list as changes occur.

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

PeopleSoft Web Financials Web Requisition

The Access Control Executive (ACE) will add Financials access at their discretion and on a “need to know” basis for users. This user will be preparing or approving online web requisitions.

1. The ACE logs into the UTHSCSA Portal
   a. HSC Business Applications
   b. ACE Tools
   c. ACE Security
   Enter a portion of the operator’s last name or complete last name and click the Search button.
2. The departmental ACE should refer to the section “Requesting and Setting up a New Operator” for detailed steps on adding Financials user access.
3. Click the SAVE option.
4. There is no mandatory training prior to granting access for the Financials application. It is recommended new users attend training.
   All necessary distribution lists and the Departmental User Security Access Confirmation Lists are updated. It is suggested the departmental ACE also update the departmental list as changes occur.

Terminating Security Access to Application Systems

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

Termination of security access to PeopleSoft, Document Review System, Data Warehouse and Hyperion is performed by the IMS Application Security team. The ACE should complete the PSAR form through the IMS Self Service portal at the time a user is terminated or transferred from the department.

The ACE should remove all PeopleSoft Financials requisition authorization roles, to include Department ID’s and Project ID’s, found within the ACE Security pages (User Access, Department Approver and Project Approver) in People Soft Financials for employees who have terminated from the department.

ACEs cannot remove access from a Principal Investigator who oversees an active grant without additional assistance from the Office of Sponsored Programs. To terminate a Principal Investigator (P.I.) from a grant Project ID (PID), the ACE should complete the following steps in order:
1. Contact the Office of Sponsored Programs (OSP) and have Sponsored Programs delete the P.I.’s user name from the Project ID. They should replace the PREVIOUS P.I. with the NEWLY appointed P.I.
2. The ACE can then remove the user name from the Project ID(s) in the ACE Tools.

Please note: The ACE can only remove the PI once OSP has completed their part and disconnected the PI from the PID or grant by replacing the “old” P.I. name with a “new” P.I. name. If the P.I. will remain on the grant, access cannot be removed.

It is the responsibility of the departmental ACE to confirm emails of a terminated employee. The ACE has 10 days to submit a service request to retain the listed accounts if it is incorrect.

Do not ignore these emails

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 the requisition authorization requests.

The major processes reviewed are:

- Review typical roles
- Review Department ID Security
- Requesting and Setting up a New Operator
- Updating an Operator Profile/Adding Access
- Updating an Operator Profile/Deleting Access

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 ID Security

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

1. Go to HSC Business Applications
   a) ACE Tools
   b) Department Inquiry

2. Log into ACE Tools and select Department Inquiry, click on the Search icon to view ALL DeptID’s the ACE owns.

3. To search for a specific department, enter a portion of the department ID and click the magnifying glass icon, or enter the full DeptID and click the Search button.

The Department Inquiry will show the ACE all Financials Requestors, Department Approvers, and Project Approvers for that department.

This is a “view only” page. To make edits to a user’s access, the ACE will go to ACE Security and search for the user’s profile.

User Access tab

The checkboxes on the User Access tab will identify the Financials access the user has:

- Requisition – if checked, the user can prepare financials requisitions
- eShip Global access – If checked, the user can ship packages for the department
- Project Budget – If checked, the user can review data for PID’s in the PBI inquiry
- Payment Request – If checked, the user can prepare or approve payment requests (This feature will not be available until the next upgrade in Summer 2016)
The ACE can also search by clicking the magnifying glass icon to view a listing of Department ID’s within the ACE’s ownership. This list can be exported into an Excel spreadsheet by clicking the download icon. Use the left and right arrows to navigate through the pages.

**Department Approver Access tab**

The checkboxes on the Department Approver Access tab will identify the Financials access the user has:

- Requisition – If checked, the user can approve financials requisitions

The ACE can also search by clicking the magnifying glass icon to view a listing of Department ID’s within the ACE’s ownership.

- Select the Dept ID then click on Search to view a listing of users who have access to that Dept ID and the user’s access.

This list can be exported into an Excel spreadsheet by clicking the download icon. Use the left and right arrows to navigate through the pages.
Project Approver Access tab

The checkboxes on the Project Approver Access tab will identify the Financials access the user has:

- Signature Authority – If checked, the user can approve paper documents
- Requisition – If checked, the user can approve financials requisitions online

This list can be exported to an Excel spreadsheet by clicking the download icon. Use the left and right arrows to navigate through the pages.

The ACE can also search by any of the following options:

- Dept ID field – Enter the Department ID or click the magnifying glass icon to view a listing of Dept ID’s within the ACE’s ownership. Select a Dept ID and click on search to view a listing of users who have access to that Dept ID.
- User ID field – Do not use this field.
- Employee Name – Enter the user’s last name or click on the magnifying glass icon to view a listing of users who have access to the ACE’s PID’s. Select the user and click on search to view PID’s they can approve on
- Click on Clear Search to clear all data from the Search Criteria box and begin a new search.
Other Information Sources

The information displayed on the Project Approver page may also be found in the HSC Self Service Inquiries within the Financials application.

The “Signature Inquiry by Project Approver” within the Self Service Inquiries link can be used to view all Project ID’s for a Project Approver regardless of department. This list of projects shows the current projects with the “Active” status.

The ACE will see the same information within the Self Service Inquiries, “Signature by Project” and “Signature by Project Approver”.

- **Signature by Project** will allow the ACE to search for approvers by entering the PID.

- **Signature by Project Approver** will allow the ACE to search for approvers by entering the name.
Requesting and Setting up a New Operator

Navigation

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 to activate the profile and assign user roles, to include Dept ID’s and Project ID’s, needed for the user to perform their job duties.

When viewing Financials access for a user, the page is broken up into multiple security access tabs in the ACE Security/ACE Tools menu. A closer view of each section is discussed in the following pages.
Section Information

Section 1 – The Header tabs

In the new ACE Security enhancements, access for a user will be broken up in multiple separate access tabs to simplify the task of granting access. Depending on the TYPE of Financials access a user needs (User, Department Approver, Project Approver), the ACE selects appropriate tab to complete the access. The ACE will only be able to add, change and delete information for the departments under the ACE’s authority.

An ACE can only unlock a NEW user profile by clicking on the yellow Add Operator button. This action will automatically unlock the NEW user’s profile and allow the ACE to add PeopleSoft Financials access as deemed necessary for the user by selecting an action from the User Access Actions section.

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 the business processes.

Additionally, if the user profile is locked, the “Add” button will be grayed out to prevent altering to the current security access set up for this profile.
Section 2 – The Action box

In the Action box, the ACE can choose what type of action (View, Add, Delete) to take for a user’s Financials access. Each tab has the Action box section; the ACE should confirm the appropriate tab based upon the type of Financials access needed.

User Access Actions box from User Access tab

Department Approvers Action box from Department Approvers tab

Project Approvers Action box from Project Approvers tab
Section 3 – The Filter and Search Criteria box

In the Filter and Search Criteria, the ACE is able to search for a listing of available options to add to the user's profile.

By typing in a portion of the Dept ID, PID, Fund or Project title and clicking the magnifying glass icon, a list of criteria that matches the parameters entered will populate in the Access Data box.

The **User tab and Department Approver tab view of this section:**

```
Filter and Search Criteria

DEPT ID

Search  Clear
```

The **Project Approver tab view of this section:**

```
Filter and Search Criteria

PROJECT ID  FUND  DEPT ID  PROJECT TITLE

Search  Clear
```
Section 4 – The Access Data box

The Access data box displays a current view of the user’s access. Click on each security access tab to see each particular type of Financials access for the user.

The User Access view within the Access Data box

The User Access tab will allow the ACE to grant user access for the following applications:

- Requisition: Checking this box **ALLOWS** the user to prepare requisitions.
- eShip Global: Checking this box **ALLOWS** the user to ship packages.
- Project Budget: Checking this box **ALLOWS** the user to run the PBI Inquiry.
- Payment Request: Checking this box **ALLOWS** the user to prepare payment requests.

(This feature will not be available until the next upgrade in Summer 2016)
To make a mass update to the user’s profile for each TYPE of access, click on either the Select All or Clear All link. This action will select/clear all checkboxes in the vertical column for Dept ID’s the ACE owns.

**BE ADVISED:** When this mass update function is used and the Select/Clear link is selected, it is not possible to revert to all the previous access the user had checked on their profile.

Click Save after any updates are selected.

Using the export feature will download an Excel spreadsheet of raw access data. The ACE should immediately name and save the data to identify which employee and type of access is exported. (For example: Smith999DeptApprvs)

This is very useful when the ACE needs to review the access for a user before the access is copied to another user.

**The Department Approvers view within the Access Data box**

The Department Approvers tab will allow the ACE to grant user access for the following applications:

- Requisition: Checking this box **ALLOWS** the user to approve requisitions.
- Payment Request: Checking this box **ALLOWS** the user to approve payment requests.

(This feature will not be available until the next upgrade in Summer 2016)

To make a mass update to the user’s profile for each TYPE of access, click on either the Select All or Clear All link. This action will select/clear all checkboxes in the vertical column for Dept ID’s the ACE owns.

**BE ADVISED:** When this mass update function is used and the Select/Clear link is selected, it is not possible to revert to all the previous access the user had checked on their profile.

Click Save after any updates are selected.

Using the export feature will download an Excel spreadsheet of raw access data. The ACE should immediately name and save the data to identify which employee and type of access is exported. (For example: Smith999DeptApprvs)

This is very useful when the ACE needs to review the access for a user before the access is copied to another user.
The Project Approvers view within the Access Data box

The Project Approvers tab will allow the ACE to grant the user access for the following applications:

- **Signature Authority**: Checking this box **ALLOWS** the user to approve paper documentation (ex: vouchers)
- **Requisition**: Checking this box **ALLOWS** the user to approve requisitions
- **Payment Request**: Checking this box **ALLOWS** the user to approve payment requests. *(This feature will not be available until the next upgrade in Summer 2016)*

To make a mass update to the user’s profile for each TYPE of access, click on either the Select All or Clear All link. This action will select/clear all checkboxes in the vertical column for Dept ID’s the ACE owns.

**BE ADVISED:** When this mass update function is used and the Select/Clear link is selected, it is not possible to revert to all the previous access the user had checked on their profile.

Click Save after any updates are selected.

Using the export feature will download an Excel spreadsheet of raw access data. The ACE should immediately name and save the data to identify which employee and type of access is exported. *(For example: Smith999DeptApprvs)*

This is very useful when the ACE needs to review the access for a user before the access is copied to another user.
Updating an Operator profile/Adding Access

Preparer Access

To add financials access to a user so they prepare requisitions or payment requests, the ACE will select the User Access tab and complete the following steps:

1. Within the Action box, click on the Add button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of available access will populate. These are available Dept ID’s the ACE has authority to add to this user’s profile. The ACE should ONLY see Dept ID’s they are owner of and the user does not currently have on their profile.
4. Within the Access Data box, check the boxes for the type of access to be added to the user’s profile.
   a. Select Requisition to allow the user to prepare requisitions
   b. Select eShip Global to allow the user to ship packages
   c. Select Project Budget to allow the user to view the Project Budget Inquiry. This access will allow the user to view key balances for a project ID without having to access the Data Warehouse application. **Be reminded:** the operator will be able to view all free balances for all Project ID’s which fall under a Dept ID they have PBI access to.
   d. Select Payment Request to allow the user to prepare payment requests (**This feature will not be available until the next upgrade in Summer 2016**)
   e. Select Inquiry Only to allow the user to view only without being in an approver role.
   f. Click Save

Department Approvers Access

To add financials access to a user so they are department approvers for requisitions, the ACE will select the Department Approvers tab and complete the following steps:

1. Within the Action box, click on the Add button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of available access will populate. These are available Dept ID’s the ACE has authority to add to this user’s profile. The ACE should ONLY see Dept ID’s they are owner of and the user does not currently have on their profile.
4. Within the Access Data box, check the boxes for the type of access to be added to the user’s profile.
   a. Select Requisition to allow the user to approve requisitions
   b. Select Payment Request to allow the user to approve payment requests (**This feature will not be available until the next upgrade in Summer 2016**)
   c. Click Save

**Please note:**
When a Dept ID is added to a user’s profile so they can be a requisition department approver, it will also insert the Dept ID on the User Access tab as “view only” so the approver can review the requisition before it is approved.
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 Approvers Access**

To add financials access to a user so they are project approvers for requisitions, the ACE will select the Project Approvers tab and complete the following steps:

1. Within the Action box, click on the Add button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of available access will populate. These are available Project ID’s the ACE has authority to add to this user’s profile. The ACE should ONLY see Project ID’s they are owner of and the user does not currently have on their profile.
4. Within the Access Data box, check the boxes for the type of access to be added to the user’s profile.
   a. Select Signature Authority to allow the user to approver paper documents **ONLY** (ex: vouchers)
   b. Select Requisition **AND** Signature Authority to allow the user to approve requisitions
   c. Select Payment Request to allow the user to approve payment requests (**This feature will not be available until the next upgrade in Summer 2016**)
   d. Click Save

**Please note:**
When a PID is added to a user’s profile so they can be a requisition project approver or signature authority approver, it will also insert the Dept ID for that PID on the User Access tab as “view only” so the approver can review the requisition before it is approved.

**Updating an Operator Profile/Deleting Access**

**Preparer Access**

To delete financials access to a user so they can no longer prepare requisitions, the ACE will **select the User Access tab** and complete the following steps:

1. Within the Action box, click on the Delete button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of current access will populate. These are available Dept ID’s the ACE has authority to delete from the user’s profile. The ACE should ONLY see Dept ID’s they are owner of and the user currently has on their profile.
4. Within the Access Data box, uncheck the boxes for the type of access to be deleted from the user’s profile.
   a) Uncheck Requisition to prevent the user from preparing requisitions
   b) Uncheck eShip Global to prevent the user from shipping packages
c) Uncheck Project Budget to prevent the user from viewing info in the Project Budget Inquiry.

d) Uncheck Payment Request to prevent the user from preparing payment requests (This feature will not be available until the next upgrade in Summer 2016).

e) Once the ACE unchecks the appropriate boxes, click on the “Delete” checkbox in front of the Dept ID to remove this Dept ID from the user’s profile.

f) Click Save

**Department Approvers Access**

To delete financials access to a user so they can no longer approve as a department approver for requisitions, the ACE will select the Department Approvers tab and complete the following steps:

1. Within the Action box, click on the Delete button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of current access will populate. These are available Dept ID’s the ACE has authority to delete from the user’s profile. The ACE should ONLY see Dept ID’s they are owner of and the user currently has on their profile.
4. Within the Access Data box, uncheck the boxes for the type of access to be deleted from the user’s profile.
   a. Uncheck Requisition to prevent the user from approving requisitions
   b. Uncheck Payment Request to prevent the user from approving payment requests (This feature will not be available until the next upgrade in Summer 2016)
   c. Once the ACE unchecks the appropriate boxes, click on the “Delete” checkbox in front of the Dept ID to remove this Dept ID from the user’s profile.
   d. Click Save

**Please note:**
If the user has no additional need to view any information for the Dept ID that was removed as a Department or Project Approver, the ACE must now remove the Dept ID role on the User Profile tab.

1. Click on the User Access tab
2. From the “User Access Actions” section, click on Delete
3. From the “Delete Department(s) and User Access section, click in the checkbox for the Dept ID to be deleted from the user’s access.
4. Click Save

**Project Approvers Access**

To delete financials access to a user so they can no longer approve as a project approver for requisitions, the ACE will select the Project Approvers tab and complete the following steps:

1. Within the Action box, click on the Delete button
2. Within the Filter and Search Criteria box, click on the Search button
3. Within the Access Data box, a listing of current access will populate. These are available Project ID’s the ACE has authority to delete from the user’s profile. The ACE should ONLY see Project ID’s they are owner of and the user currently has on their profile.
4. Within the Access Data box, uncheck the boxes for the type of access to be deleted from the user’s profile.
a. Uncheck Signature Authority to prevent the user from approving paper documents (ex: vouchers)
b. Uncheck Requisition to prevent the user from approving requisitions
c. Uncheck Payment Request to prevent the user from approving payment requests (*This feature will not be available until the next upgrade in Summer 2016*)
d. Once the ACE unchecks the appropriate boxes, click on the “Delete” checkbox in front of the PID to remove this PID from the user’s profile.
e. Click Save

**Please note:**
If the user has no additional need to view any information for the Dept ID that was removed as a Department or Project Approver, the ACE must now remove the Dept ID role on the User Profile tab.
1. Click on the User Access tab
2. From the “User Access Actions” section, click on Delete
3. From the “Delete Department(s) and User Access section, click in the checkbox for the Dept ID to be deleted from the user’s access.
4. Click Save

### 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 for processing through the IMS Self Service Portal. If the user already has access to DW, the HR Pay Listing security access role will be added to the user’s profile in Active Directory.

1. Complete the PSAR form by checking off the HR Pay Data radio button.
2. In order to have access to HR Pay Data reports, the user will need a DW License. If the user is not a current DW user, the ACE will need to identify an employee to transfer the DW license from. If the user currently has a DW license, the ACE should enter that information in the comments section.

![Add DW Access](image)

Has the user attended mandatory DW Training?
- Yes
- No

Does the user have an existing DW License?
- Yes
- No

Does the user need access to HR PayListing Report?
- Yes
- No

DW add access comments

After the ACE receives a confirmation email via Supportworks, the ACE will need to complete the following steps.
1. Go to HSC Business Applications
2. ACE Tools
3. Data Warehouse Security
4. Enter the operator’s domain username or a portion of the operator’s last name and click the **Search** button. Select the correct user for the access to be added.
5. To add a new Department ID for this user, click the plus sign \(+\) or the minus sign \(-\) to remove a department.

6. The HR checkbox must be selected for each department ID added for the user. This action will complete the permissions for access. If this checkbox remains unchecked, the user will NOT be unable to view and run the HR Pay Listing Report.

7. 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 a requisition.

Below is an example of the email notification sent to the requester, contact person and any additional persons listed.

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.

To add a user to the PO Notification process, the ACE should complete the following steps:

1. Go to HSC Business Applications
2. ACE Tools
3. PO Dispatch Notification Email
4. Enter the Dept ID or the first letter of the Dept ID and click the Search button.
5. Type in the UTHSCSA e-mail address of the person(s) who should receive the PO notifications.

6. 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 requiring intervention from Application Security

The departmental ACE is still required to send an email request to the Application Security 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 Application Security 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 Application Security team for processing through the IMS Self Service Portal 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
  Persons of Interest do not automatically have a profile created because they are not actual employees at UTHSCA.