FIRST

(This page is intentionally left blank for printing purposes.)

User

W* nBT/F8 9.96 Tf96 Tf1 0 0 1 534.34 288.77 Tm0 g0 G 0.0101 Tc[(..........3(0.0101 Tc[(.........)] 8 241.25 240.65 Tm0 g0 G[( )] TJET....

Some business processes require only one role to complete. More complex business processes, such as running a pay cycle under Accounts Payable, may require multiple roles to complete. Our granular approach promotes flexibility across institutions and reduces the risk of segregation of duties issues. ITS designs and creates the roles and permission lists and allows institutions to administer the delivered roles to their individual users through a distributed user profile. We will cover this more in the security administration area of this document.

Dynamic Roles

To make role assignment faster and more efficient, the Georgia**FIRST** model utilizes the dynamic roles functionality within PeopleSoft. Dynamic roles allow administrators to assign roles based on preset permissions.

Roles can be assigned dynamically using several different methods. One method is by creating a query that says, If a user has access to role X, then automatically give them role XX as well. In addition, if a user has access to page X, then role X can also be assigned. The benefit of creating a dynamic role is that, when role X is removed, role XX is also removed. Queries, PeopleCode, or Directories can be used to assign dynamic roles.

Currently, ITS has only one Dynamic Role: the BOR_EX_APPROVAL role. Any user who is on the Expenses Approver Assignments page automatically gets this role. As a result, they also receive permission to approve expense transactions. Upon termination, the user should be removed from the Expenses Approver Assignments page. The Dynamic Role will automatically be removed from their user profile.

Permission Lists

Permission Lists, building blocks of end-user security authorizations, control what a user can and cannot access. A user inherits permissions through the role or roles the security administrator assigns to them. In the chart above, notice that permission lists are assigned to roles, which are then assigned to user profiles. A role may contain numerous permissions and a user profile may have numerous roles assigned to it. Because permission lists are applied to users through roles, a user inherits all the permissions assigned to each role to which the user belongs. The user's access is determined by the combination of al

permissions, the smaller the number of permissions within a particular permission list, the more flexible and scalable that permission list is.

Please note: Data permissions are assigned directly to the User Profile either through a Primary Permissions list or Row Security Permissions list (this will vary in HR or Finance). Navigator Homepage and Process Profile permission lists are also assigned directly to the user profile.

All permission lists start with the module, i.e., GL for General Ledger, and are

System security involves protecting financial data against modification, loss, theft, and unauthorized disclosure. To ensure the safety of data, Georgia**FIRST** has a security framework with several key

User Profiles define individual PeopleSoft users. You begin the security process by defining User Profiles and then linking each User to roles. Normally, a User Profile is linked to at least one role in order for it to be a valid profile; however, it is possible to have a User Profile with no Roles if, for example, a user who is not allowed access to the PeopleSoft application needs to receive workflow-generated emails. As we explained in the Introduction, the majority of permissions (values) that make up a user profile are inherited from the linked roles.

User Profiles

The first thing you must do to set up a User Profile is create a User ID by entering appropriate values, such as user pass0000912 0 612 792 reW* nBT/F1 11.04 Tf1 0 0 1 67.584 60R.T/F3JETQq0.00000912 0 612 792 reW* G[(such)5(as)9(u

kflo

characters: ; : & , < > \ / " [ ] ( ). People Tools version 8.5+ allows you the naming length of up to 30 characters. (Some institutions prefer that the User ID not be tied to the user's name. Check your institution to see if they have a preferred style for User IDs.) Click the Add button.

The second way to create a new Profile is to use the Copy User Profile feature to duplicate a similar profile. The benefit of using this method is that, if you have a core user with 50 roles and hire another user who needs the same 50 roles to replace them, you either have to manually add the 50 roles or do the Copy User Profile, which copies the roles. To copy a User Profile, follow the navigation: **PeopleTools > Security > User Profiles >** Copy User Profile. The name of your new profile will need to be different from the one you are about to copy.

Please note: The third way to create a User Profile is to have the user self-register. This method is explained on page 24.

The only other fields that may be required on the "General" tab are the Process Profile and Primary fields in the Permission Lists portion of the page.

Permission Lists

The Process Profile can control which processes a user is allowed to run. In the GeorgiaFIRST model, processes are not grouped into different process groups. If a user has security to a page, he or she can run the process because all processes have been consolidated into one group. To add a process, type PT_PRCSPRFL into the Process Profile.

Please note: This is the only instance where a permission list is attached directly to the User Profile.
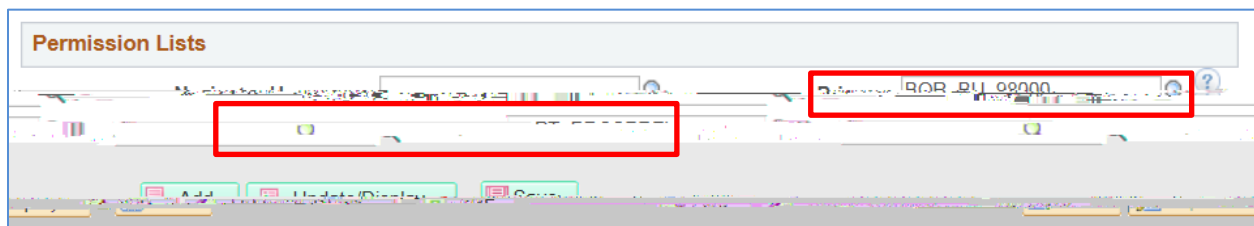
The Primary permission list is what controls which institution's data the user can access, update, and inquire on. For example if a university's Business Unit is XXXXX, the user's primary permission list is BOR_BU_XXXXX. This list enforces row level security and allows users to see data only from their institution. To give permission for a Primary level,

1. Click on the Search symbol beside the Primary key field.
2. Click the number that corresponds to your organization.
3. Click Add.

If the local security administrator creates the profile manually, the process profile defaults from the local security administrator's profile.

The next tab on the User Profile is the ID tab. This tab is used to set the ID type for the user. For end users who are employees, this will be set to Employee.
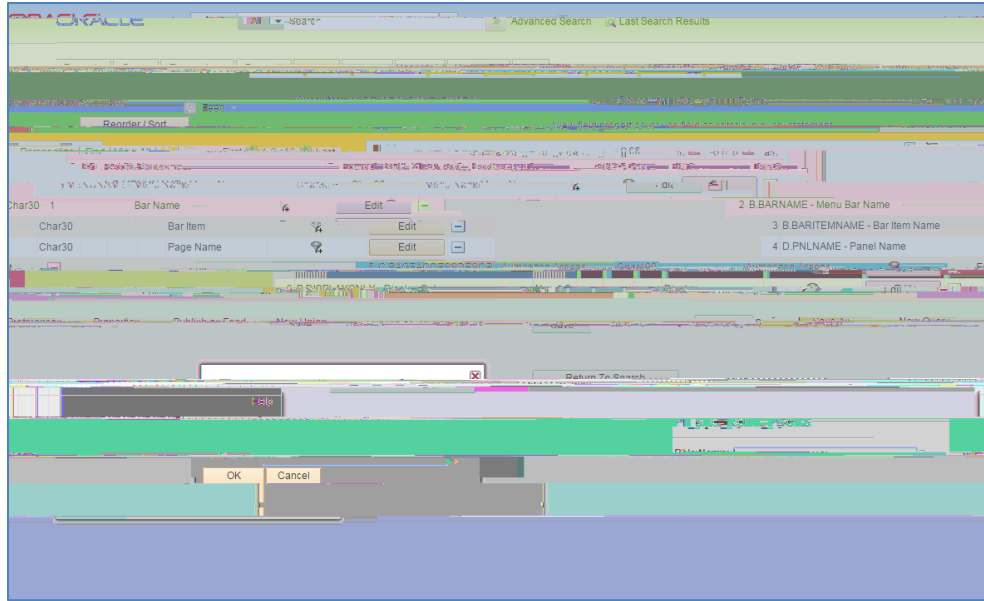
Click run and enter your search criteria. Select OK.

PT SEC ROLE PAGES

Role Name: BOR_AP_INQUIRY

OK   Cancel
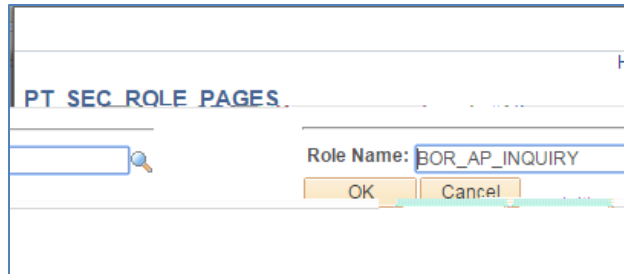
You have a request to add security to a user and this user needs to be able to enter a voucher.

1. What role should you give them? _____

2. Are there any other considerations you need to look at for this user? If so list them here:

   _____

You have another request for a user to be able to Run depreciation on an asset.

3. What role is required? _____

Institution-Specific Job Aids and Forms

As discussed before, one of the best ways to determine what access your employees need is to create custom security job aids by job functions. The GeorgiaFIRST website has sample job aids (http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security); however, job functions will vary across institutions. Look for common job titles between various departments at your institution. Then if the job duties are the same, or even have only a few exceptions, document the security for that job duty and note the exception roles and preferences. As new hires come along and are placed in those job functions, you will have the security assignments documented.

For instance, some institutions have a directory on their campus website that lists each department and may also include names and job titles. If your Budget Office has a Director, Assistant Director, and Budget Analyst, for example, you could look at the job functions for each and determine what security requirements are needed and document them. It may be that the Director and Assistant Director need the same security, so only one job aid would be needed. If only a few roles differ, you could use the same job aid and note the differences. The Budget Analyst would not need as much security, however, so I would expect to see a different job aid for t-3(ac 612 7sire)<IfCID

General Ledger transactions need to go to a different approver than the ePro transactions, use the Monitor Worklist page to reassign these transactions individually.

One other point to consider is that, reassigning work can cause issues if

3. Fill in the required fields on the next screen:

4. The system will display the job row for the employee who is self-registering. They need to click the box beside the active job row and select next. At this point, the user can create his or her own User ID and setup a password and email address. At this point, registration is complete. They have to sign out and sign in with their newly created user ID and password.

This provides the employee with basic sign-in rights, and if their institution uses expenses, it assigns the basic expenses access required to create and print expense transactions. No security form is required for self-registered individuals until they need additional roles. At that point, approvals and documentation are required.

1. Login to FPLAY with your User ID and password that you use in current production.
2. Create a new User ID and assign it the following roles: BOR PeopleSoft User, BOR_FN_ADMIN_REPORTING,

Each functionality in PeopleSoft Financials System relies on every user having access (and not having access) to

The first General Preference, the Overall Preference, is the business unit/setid and is required. Entering this information defaults the business unit on all user transaction pages. For example, in General Ledger, when a user adds a journal entry, the business unit defined here will default on the journal entry so that the user does not have to enter their institution ID for each transaction.

1. Enter the User ID and Name fields default.

2. Enter the default Business Unit

3. Enter the default SetID field.

4. As of Date displays the default date for the Combo Edit process.

5. Enter "USA" in the Localization Country field.

6. Do not select

The second choice is Process Group. This is set up by Security and controls the on-demand features on transaction pages. For instance, a user who enters a voucher may want to run budget check and voucher post directly on the voucher entry page. This transaction would be controlled and enabled through process groups. The Allow Processing checkbox must be selected.

Once you click Save, you will see a list of process groups that are enabled for different source transactions within the system. (You can also copy these source transactions from another user.)
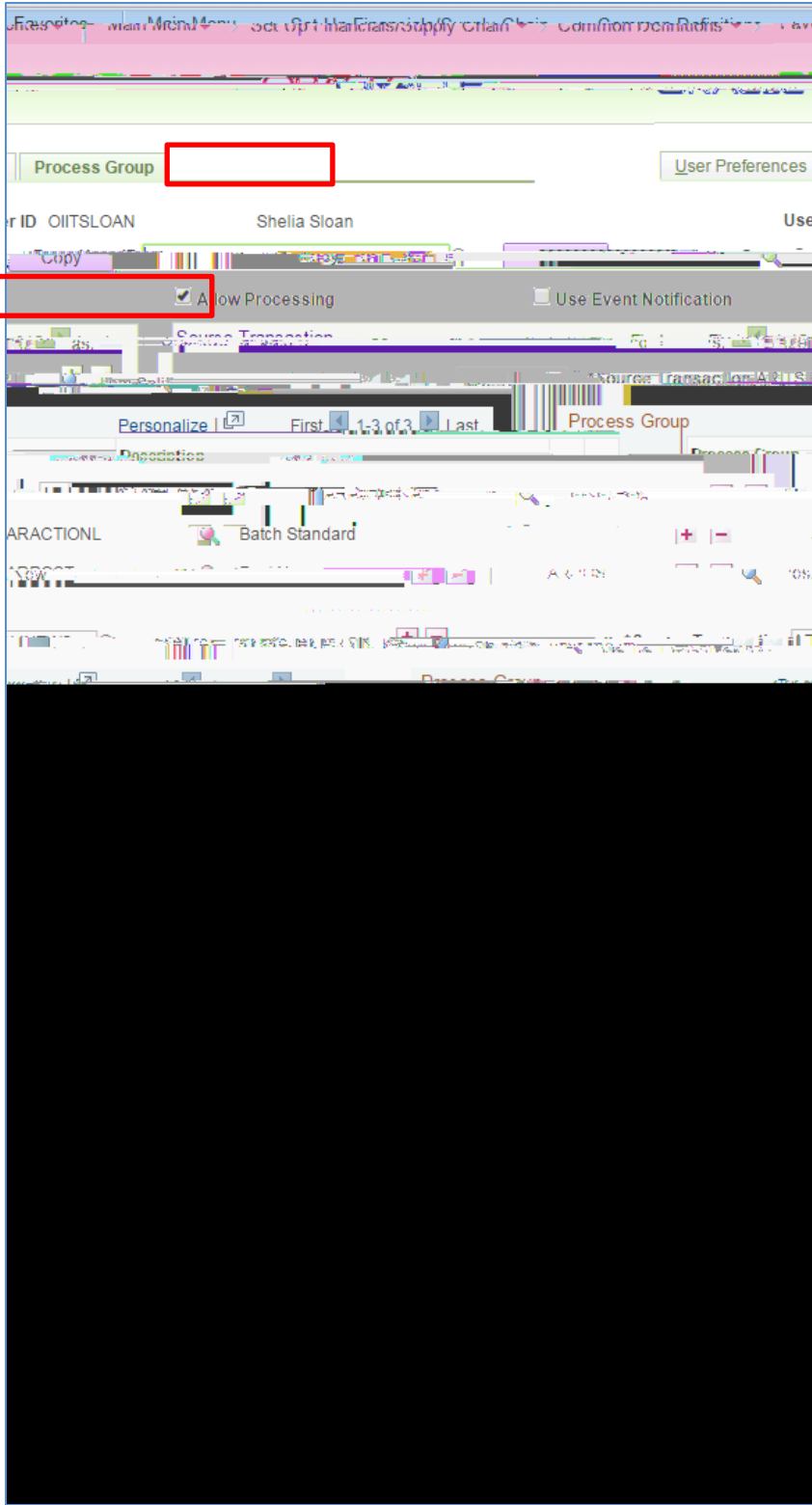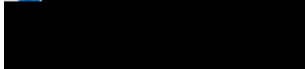
User

If you are an Asset Management User, you need to make sure that your security administrator has given you the following options:

1. Select a drill-down group to be used by online reporting when filtering data.
2. Supply a default date on which you want this transaction distributed to the general ledger. The accounting date is validated against the open periods that you establish for Asset Management in the FIN_OPEN_PERIOD table to determine to which period the system posts. (The difference between the transaction date and the accounting date determine whether any prior period depreciation must be calculated. For example, suppose that a computer was acquired and placed in service on 3/16 but was not entered into Asset Management until 8/1. All general ledger periods prior to August are closed. In this case, Asset Management automatically calculated depreciation starting in March and posts it to the general ledger in August.)
3. Click on Asset Management Integration to add transactions from Maintenance Management to the transaction loader process.
4. Under Edit Options for Interface Table, choose the following information:
   o Edit Financial Information:
      ALL: Select to allow this user to make edits to all financial transaction table entries.
      Date: Select to allow

and the journal reedited, inconsistencies between the subsystem data and the general ledger data can be created.

4. Enter Adjustment Type Journal: Select to allow a user to enter a book code adjustment type journal.

5. Save Journal Incomplete Status: This option enables the user to save journal entry transactions with an incomplete status and prevents them from being edited or posted until they are complete.

6. Allow GL Entry Event Bypass: Select to enable the user to bypass selecting entry events in PeopleSoft General Ledger journal entry, even if they are required on the Installation Options–Entry Event page.

Online Journal Edit Defaults

Procurement

To work with the Procurement module, return to User Preferences and click on Procurement under Product Preference.
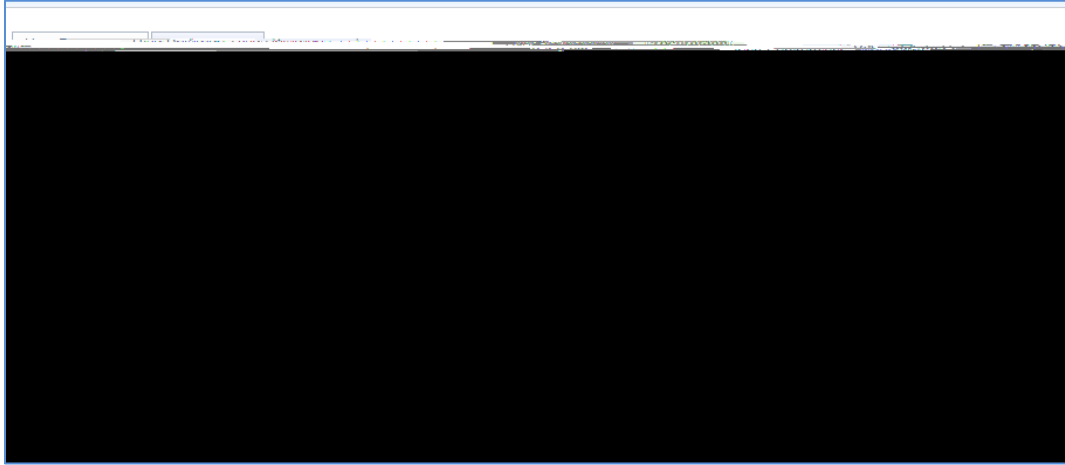
1. Enter the User and Name default.

2. Enter the default Location where requested items should be delivered when they are received.

3. Enter the default Origin.

4. Enter the Department (optional).

5. Enter the Ship to Location (optional).

6. Enter the Requester: This is Required if the user is a requester.

7. Enter the Buyer authorized to enter Purchase Orders (PO's) (optional).

8. Click the Save button.

9. Select the Payables Online Vouchering link.

1. Enter the User ID and Name default.

2. Default Values: Select a voucher Origin.

3. Operator Voucher Authorities

   o Pay Unmatched Vouchers: This gives users the authority to pay vouchers that have not been matched up to the maximum amount that is specified in the Pay Unmatch Amt f
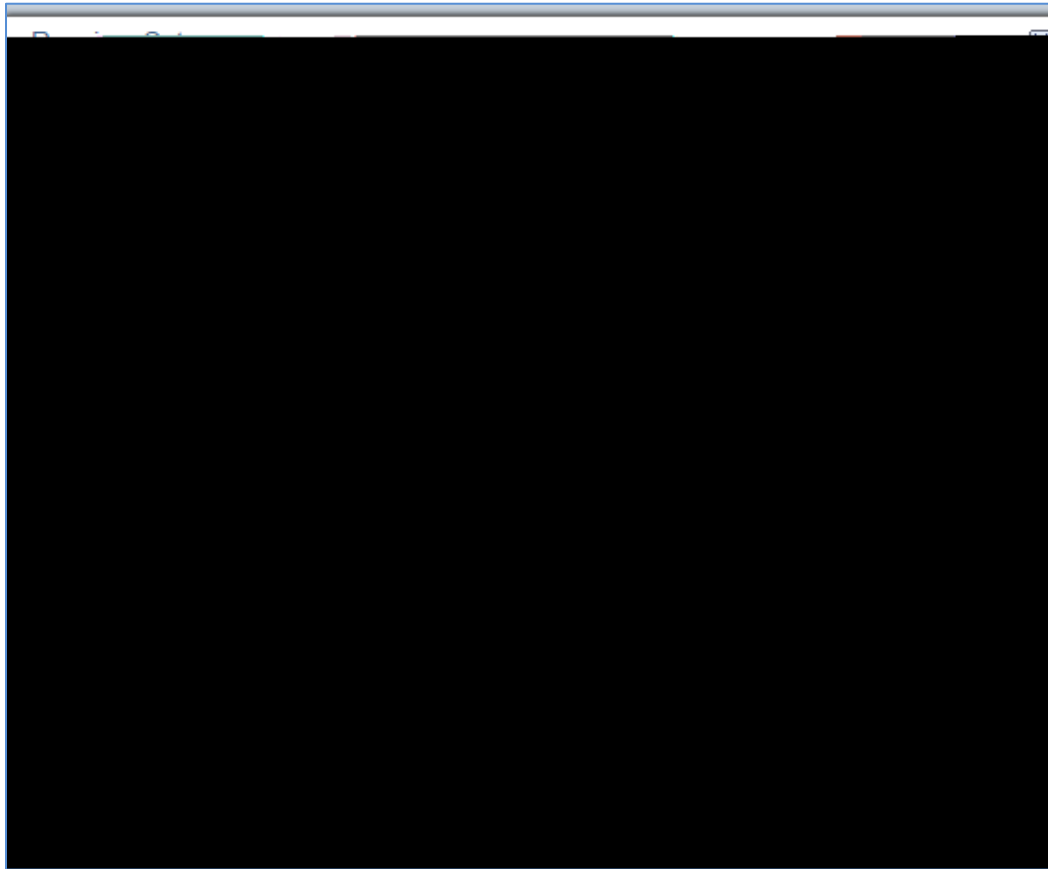
o   Security for Voucher Styles: Click to access the Voucher Styles page. The selected voucher style defines authority for each of the voucher styles checked.

Select the appropriate authorized voucher styles based upon responsibilities.

Click OK.

Receiver Setup

1. Enter the User and Name default.

2. Change Non PO Receipt Price: Select to enable the user to change the receipt price for an item on a non-purchase order receipt.

3. Interface Receipt: Select to automate the passing of inventory and asset information through the Receiver Interface Push process.

4. Run Close Short: Select to call the close short process automatically during the receiver interface push processing.

5. Subcontract Streamline: Select this check box if you want the subcontract streamline check box to appear selected by default for a subcontracted purchase order receipt for this user. The user will be able to override this field setting for a subcontracted purchase order receipt. The system determines whether to perform subcontract streamlining (purchase order receipt and production completion for the production ID in a single step) from the receipt. Streamlining processing for subcontract RTVs enables you to process RTVs if the completions have been performed on the associated receipt. The

User's Guide for

Often collaboration must take place between procurement personnel and another group before a

wa

express functions. The user must use the Inventory Express Issue component to issue inventory returns that are being shipped to the vendor.

13. RTV Inventory Destroy Options: Select the return to vendor destroy option that you want to use as this user's default value for the Inventory Process field on the RTV line. This option is only used by the RTV function when the disposition on the RTV line has a value of Destroy. The system determines the destroy option default value first by checking the user preference destroy option. If the user preference value is **Manual** or **Express**, then the system uses that default value. If the user preference value is **Default to Business Unit,** the system uses the destroy option defined at the business-un I 1 242.09 5 sT2W* n(Des)8(tr)-4(o)5

Purchase Order Authorizations
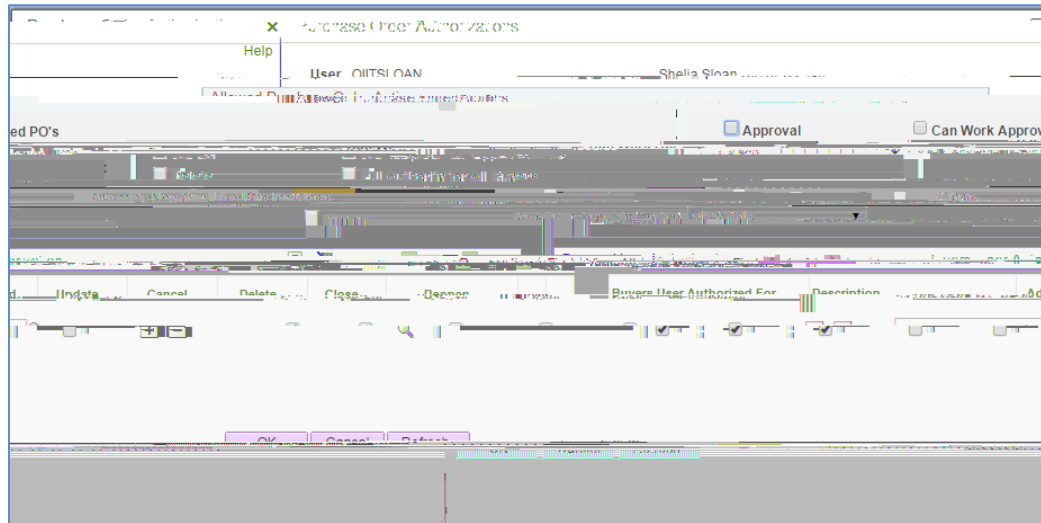
1. The User and Name default.

2. Can Work Approved POs: Select to change a purchase order that has already been approved or dispatched.

3. Can Dispatch Un-Approved POs: Select to enable a user to dispatch purchase orders with a status of pending approval.

4. Full Authority for All Buyers: Select to add, update, cancel, and close purchase orders for all buyers

5. Override Non-Qualified POs for Close: Select to close unqualified purchase orders.

6. Enter " †   \   ' for the Rebate ID Security Control.

7. Select Approval if the user is Purchase Order Approver.

Buyers User Authorization (Optional)

1. Enter Buyers User Authorized For the buyers for whom this user can enter purchase orders.

   o   Select ˚   , y   , #   , #   and k   only if the full authority is not selected.

2. Click OK

3. Select the Vendor Processing Authority link.

Workflow Administration

Each Institution needs one or more Workflow Administrators. They are responsible for Routing Management and Transaction Rerouting. Transactions missing approver assignments or transactions that have escalated due to no approvals will need to be redirected to the appropriate approvers by the administrator. Escalation and Notification Days are configured by Module and can be institution specific.

Each institution must determine the number of days workflow has to notify the approver that they have not approved the transaction and the number of days before it escalates the transaction to the Workflow Administrator.

Approval Roles vs. Routing Roles

We discussed this process in the Introduction; however, it is important to mention it here as well. Because many types of roles exist, approvers will need permission for several different roles to be able to facilitate various types of approvals and workflows. An Approval role, i.e., BOR_EP_REQ_APPROVE, contains the pages in the system where the approver would go to approve the transaction. However, workflow needs to know who to route the transactions to. There are several ways to configure this. One way to route a transaction is by role. This role, i.e., BOR_ASSET_APPR, has no page access and no permissions. It is used by workflow only for routing pui0.000009Tu10(used

User's Guide for

change will not take effect. (If you forget to run the request build process, the BORBATCH process that runs every night will run it for you.)

1. Login to FPLAY with your User ID and password from fprod (not the one you created).
2. Navigate to PeopleTools > Security > User Profiles > Distributed User Profiles. Create a Payables User ID with the following roles: BOR PeopleSoft User,

BOR_GL_TIGA_PROCESSING	TIGA Processing	This role allows users to process data for the Transparency in Government Act.
BOR_QRY_SENSDATA	Query Sensitive Data	This role allows access to employee sensitive data included in queries and reports.

Budget Preparation (Budget Prep)

Each year, University System of Georgia institutions complete the development of their proposed budgets for the upcoming fiscal year. This process includes the budgeting of personal services, fringe benefits, and non-personal services

Check imminent future financial obligations (pre-encumbrances and encumbrances) against control budgets.

Check recognized revenue against revenue estimate budgets.

Please note: A user must be tied to an employee ID to be selected on this page.

Below are the available rules, Budget Date Override, Budget Override, and Bypass Budget broken out by module, as well as two rules that were part of the 9.2 upgrade: BUD_ENTRY (enter budget journals) and BUD_XFER (enter budget transfers only). If a user needs

ITS has implemented an optional Workflow for Commitment Control Budget Journals. Institutions wishing to implement this workflow need to give their approvers the BOR_KK_BUD_APPR role. In addition, someone at the institution will need the BOR_KK_ADMINXX role (first two digits of institution ID) for escalations or routing issues.

1. Login to FPLAY.gafirst.usg.edu with your fprod User ID and password.
2. Use the Buyer User ID you created above. **** Use Activity 1 User ID instead.
3. Navigate to Commitment Control > Define budget Security > Assign Rule to User ID.
4. Give them the BUDG_DT_PO, BUDG_DT_RQ, OVRD_PO and OVRD_RQ rules.
5. Then you must run the _____ process.

Expenses

The Expenses Module allows employees to enter expense reports, travel authorizations, and cash advances for travel-related purposes. Basic self-service access can be granted by self-registering for a user account, which allows travelers to login to the self-service portal from anywhere and complete their expense reports. The Base role of a BOR PeopleSoft User contains expenses access in self-service for expense reports and travel authorizations. (Cash advances are administered via a separate role.) If your institution chooses not to use travel authorizations, the base role would be BOR PeopleSoft User–no tauth. If your institution doesn't use expenses at all,

It is important to note that with Expenses and some of the other modules, many employee notifications are sent to the email address listed on the User ID of the employee. Therefore, the Email checkbox on the User Profile, Workflow tab must be selected for the individual to receive notifications.

As with Accounts Payable, you must check user's commitment control rules for Expenses. If your user needs to overrid41.304 Tmtr us 612 792912 0 612 792 reW* nBT/F1 11.04 Tf1 0 0 1 401.83 704.98 Tm0 g0 G[(m)-4(an)15(y)] yid41.

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access
BOR_AD_HOC_APPROVE	Enables the Buyer to insert additional approvals into the Workflow when necessary
BOR_EP_REQUESTER	Enables the Buyer to create their own requisitions
BOR_EP_BUYER_CENTER	Enables the Buyer to access the Buyer Center in order to expedite requisitions
BOR_EP_INQUIRY	Enables the Buyer to run inquiries on requisitions
BOR_EP_PROCESSES	Enables the Buyer to run requisition processes
BOR_EP_REQ_APPROVE	Enables the Buyer the ability to approve requisitions that are assigned to him/her
BOR_PO_REQ_WORKBENCH	Enables the Buyer to use the Workbenches for requisitions
BOR_PO_INQUIRY	Enables the Buyer to run inquiries on purchase orders
BOR_PO_MAINTAIN	Enables the Buyer to perform maintenance on existing POs
BOR_PO_PROCESS	Enables

1. Select the Add a New Value tab.

2. Enter the buyer's User ID in the Buyer field.

3. Click the Add button.

1. Ensure the status is set to Active.

2. In the Department SetID field, enter/select your institution's SetID.

3. If the b

4. In the ShipTo SetID field, enter/select your institution's SetID.

5. In the ShipTo field, enter/select this Buyer's default Ship to location.

6. In the Location SetID field, enter/select your institution's SetID.

7. In the Location field, enter/select this Buyer's primary location.

8. In the PO Origin SetID field, enter/select SHARE.

9. In the Origin field, enter/select ONL.

10. If desired, enter a phone and fax number.

11. Set the Default PO Status to Pending Approval/Approved.

12. Click the Save button.

Please note: If the Buyer will also be creating Requisitions, they must be set up on the Requester Setup Page also. See ePro chapter below.

Receiving can be configured to "do not receive", "optional" or "required". Users can take advantage of desktop receiving or use the traditional way of central receiving. The user role for Receiving through Purchasing is BOR_PO_RECEIVING. If users want to use desktop receiving, they must have the BOR_PO_RECV_EPRO role.

ITS has reduced the number of roles associated with Supplier activity and controlled it with user preferences. Now there are only two user roles: BOR_PO_VENDORS_APPROVE and BOR_PO_VENDORS_MAINT. Security administrators can control what actions the user takes on the supplier through user preferences. For instance, if you want a user to be able to modify an existing supplier but not add a supplier, they would get the BOR_PO_VENDORS_MAINT role, but not the Add User Preference. See more details in the User Preferences section above.

In 9.2, Purchasing workflow changed from using Route Controls to using the Approval Framework. The approval role for Purchase Orders with Budget Reference differences is BOR_PO_BUD_REF_APPR. The approval role for Purchase Orders with Asset Issues is BOR_PO_ASSET_APPR. The role for escalations or routing issues is BOR_PO_ADMINXX (XX is the first two digits of institution ID). Keep in mind that these three roles are used only to route transactions to users. They do not contain page access. An approver will also have to have the BOR_PO_APPROVE role to approve a purchase order at any of the above levels. This role ETQr 1 424.99 120.(This)] TJleve

The eProcurement module features many different security components. Not only does it have Regular Page Access roles and Workflow Roles, but it also has Role Action roles. The Security Job Aids by Job Functions outline many of the ePro roles and responsibilities, and the Workflow Stage Documents explain the workflow options as well.

Types of Roles Involved

For the ePro and Georgia**FIRST** Marketplace functionality to work properly, users are set up with specific roles and responsibilities. They include:

> Shoppers: These users select items in the Georgia**FIRST** Marketplace.
>
> Browsers: Users without any Georgia**FIRST** Marketplace roles assigned will default to a Marketplace Browser. Browsers can view items, contracts, and prices in the Marketplace but cannot shop or create requisitions.
>
> Requesters: These users take the shopping carts created by Shoppers and turn them into ePro Requisitions or build their own shopping carts.
>
> Approvers: These users are set up to approve ePro requisitions.

1. Ensure the status is set to Active.

2. In the ShipTo SetID field, enter your institution's SetID.

3. In the ShipTo field, enter/select the default Ship To address for this Requester.

4. In the Location SetID field, enter your institution's SetID.

20. In the SetID field, enter/select SHARE.

21. In the Catalog ID field, enter/select NIGP_TREE.

22. Leave the Use Only Assigned Catalogs checkbox blank.

23. Save the page.

Don't forget to set up user preferences as well. These were defined in an earlier user preference section. You also have buyer set up to complete, but we will cover that in the next section, which is covered in the Purchasing section of the previous chapter.

A critical component of

User's Guide for

User's

User's Guide for

the basic security roles, along with their specialized approver role (i.e., BOR_IT_APPR for your institution's IT approvers). **The** Basic Approver Security Roles are as follows:

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access
BOR_AD_HOC_APPROVE	Enables the Approver to insert additional approvals into the Workflow when necessary
BOR_EP_REQ_APPROVE	Enables the Approver to approve/deny requisitions
BOR_EP_MAINT_REQ or BOR_EP_MAINT_REQ_SCI	Enables the Requester to edit and track requisitions in the system. If your institution is implementing the Georgia**FIRST** Marketplace, use BOR_EP_MAINT_REQ_SCI. If your institution is not implementing the Georgia**FIRST** Marketplace, use BOR_EP_MAINT_REQ.

Special Item Approver Security Role3(o)5(I)-3(e)14(3(o)5(I)-3(e)14(3(o)5(I)-3(e)14(3(o)5(I0.31 Tm0 g0 GA-.584 498.91 0.9

Role Name	Purpose
BOR_EP_RA_CHANGEALL	Allows the Approver to update any portion of the requisition without restarting Workflow on requisitions that are not fully approved. If the Requisition has been approved and the approver makes a change, the requisition will re-route back through Workflow.

When updating the Department ChartField, you need to make sure that the department's status is "Active". When you complete the Manager ID field, the Manager Name field should populate as well, once you tab out of the field. To update a department manager ID, follow the navigation: Set Up Financials/Supply Chain > Common Definitions > Design ChartFields > Define Values > ChartField Values > Department.

1. On the Find an Existing Value page, enter/select the Department ID in the Department field.
2. Click the Search button.
3. Select the Department you want to update.

1. Ensure the Department status is Active.
2. Click the Correct History button.
3. Select the Manager ID look up icon.

For a user to run a query, they must have authorization to access the records behind the query. Most records are included in the role BOR_PT_QRY_ALLACCGRPS. However, certain records have been broken out into other roles for sensitive data considerations. BOR_QRY_SENSDATA and BOR_PT_BUD_PREP are examples. If a user tries to
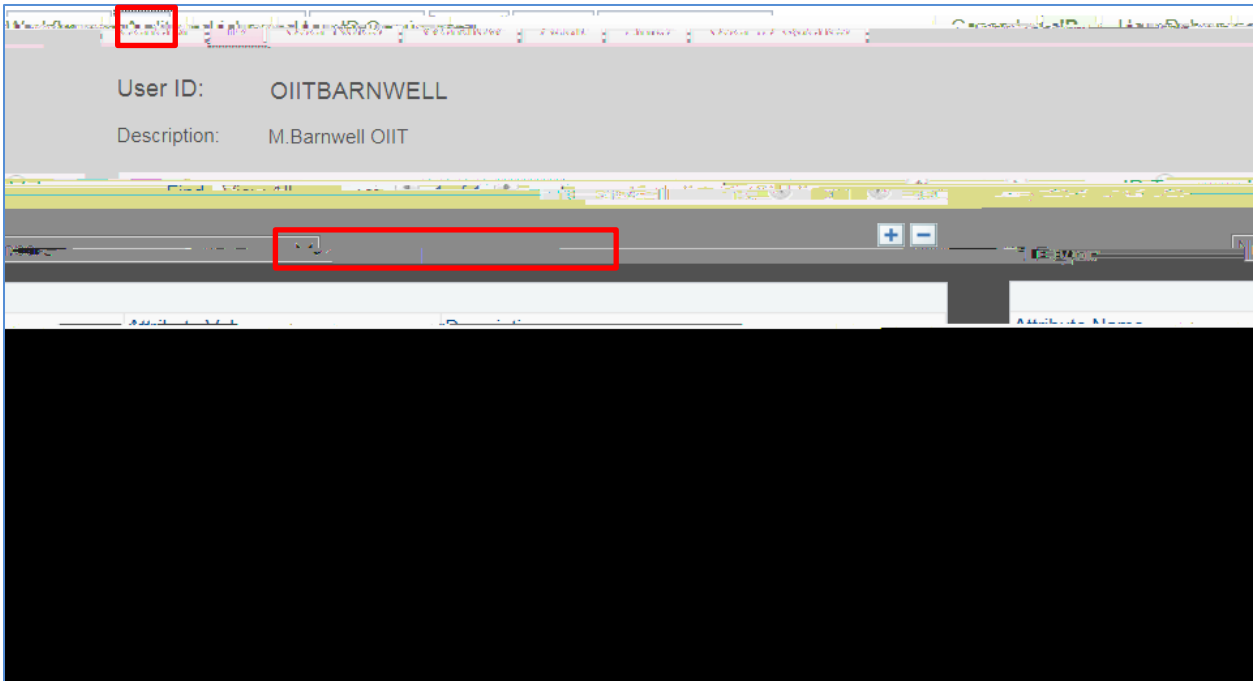
4) Place the employee ID on the General tab under the User ID alias field and attach the User ID beside it.
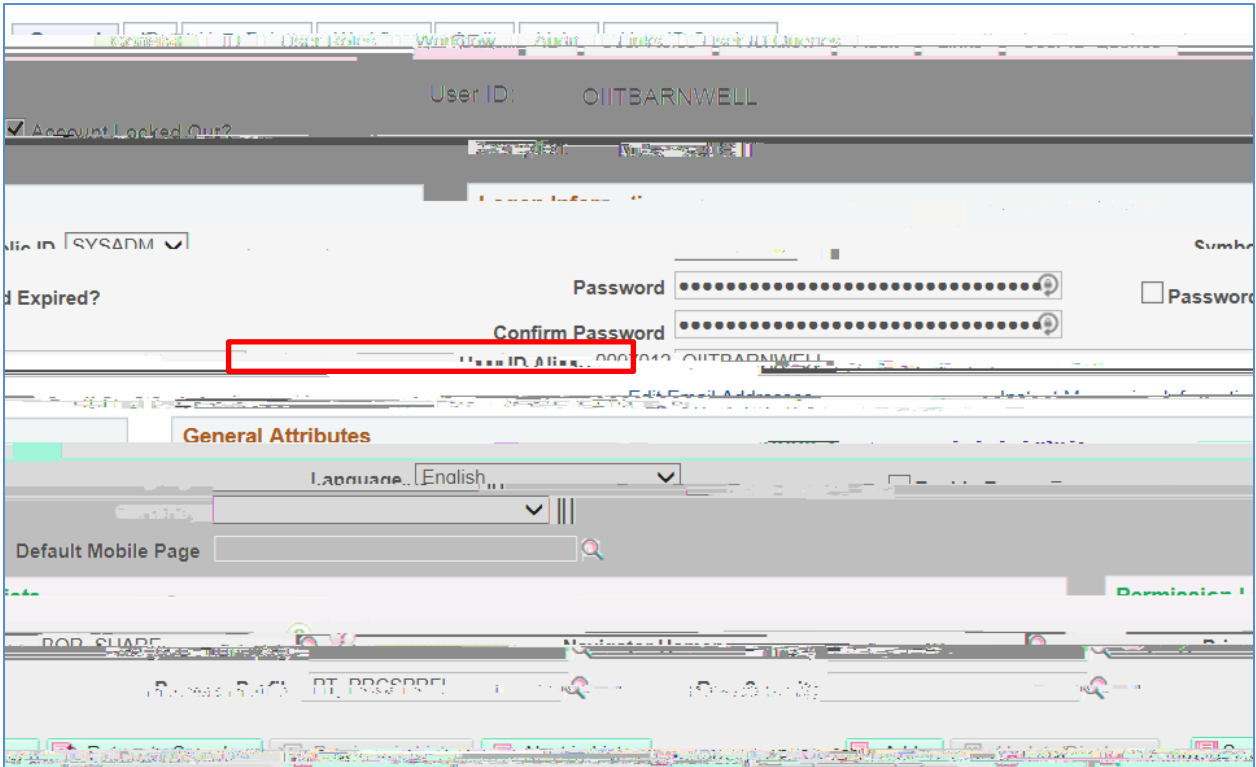
5)

Login to fplay using your prod user name and password.

1. Go to the Query Manager under Reporting Tools and run the BOR_TERMINATED_USERS_QUERY.

2. Follow the procedures above if you have any results on the query. Pick only one user.

User

Login to fplay using your prod user name and password.

1. Go to the Query Manager under Reporting Tools and run the SEGREGATE_DUTY_BOR query.

2. Choose Create Requisition.

3. Make note of user.

Login to fplay using your prod user name and password.

Go to the User Preferences Report and run it for ALL Products and for User ID noted in Activity 11.

To run the Commitment Control Security report

Category	Description of Change/Update	Frequency	Completion Date Range	Completion Date
Account Setup/Termina98 00.4				

User's Guide for

A. The issue is that the User ID is not setup as employee. IT must contain an employee ID to receive commitment control security.

Q. What role allows a user to do only password resets?

A. The role name is BOR_PT_USER_GENERAL. This can be given to a helpdesk to have them do the majority of the password resets.

Q. When I click save to reset a password for a user, I get a multi-campus user error.

A. Sometimes people define an alternate user and forget to remove it after the date range expires. If this

A.0134 Tc[(Q.)] TJETQg0.00000912 0 612 792 reW* nBT/F2 11.04 Tf1 0 0 1 78.144 564382. da0 g0 G[(a)] TJETQg0.00000912 0 612 792 re