Modify Requester LOV

Sample Use Case: Restrict public persons to only those who belong to the same BU as the BU in the primary work assignment of the logged in user.

Introduction:

Public Person records are records that all workers have access to. For example, Preparers while creating requisitions, can search the Requester LOV to pick a user that they want to order items for. Self Service Procurement users can also search the Requester LOV to pick people that they want to reassign a requisition to. Typically, the Requester LOV gives access to all those with an active primary assignment record.

It is possible to restrict the records returned in the Requester LOV i.e. to stop it from returning everybody with a primary active assignment record. In this document, we will show how to only return users who belong to the same requisitioning BU as the BU of the primary work assignment of the logged-in user.

Step 1: Duplicate the seeded Procurement Requester, Procurement Preparer, Advanced Procurement Requester and Employee roles

Security Console > Employee > Copy > Copy top role and inherited roles

Note:

a) At the minimum, you need to duplicate the Procurement Requester and Employee roles

   Employee role inherits Procurement Requester role by default.

b) If you use Procurement Preparer and Advanced Procurement Requester roles in your organization, then duplicate those too

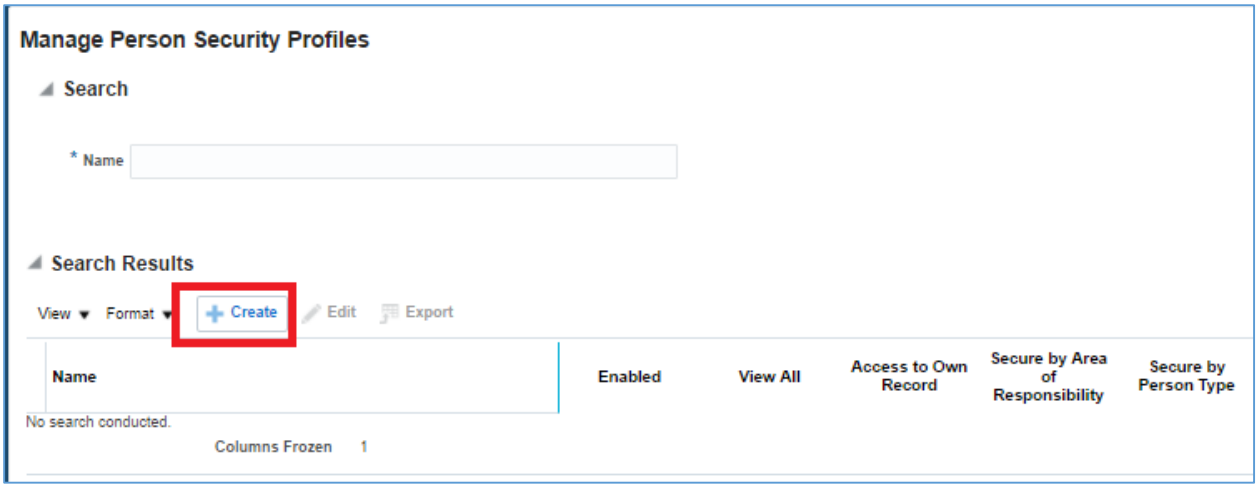
   Procurement Preparer inherits Procurement Requester role while the Advanced Procurement Requester inherits the Procurement Preparer role

Tip:

a) Duplicate the Employee role first and if you choose ‘Copy top role and inherited roles’, it will also duplicate the Requester role

Step 2: Create a custom person security profile

Setup and Maintenance > Manage Person Security Profiles



Tick the 'Secure by Custom Criteria' checkbox and enter the SQL below

Note: First copy the SQL to Notepad, save it and then copy from Notepad into Oracle Application or directly type in the SQL into Oracle Application. Copying from Notepad ensures the characters are in Unicode.

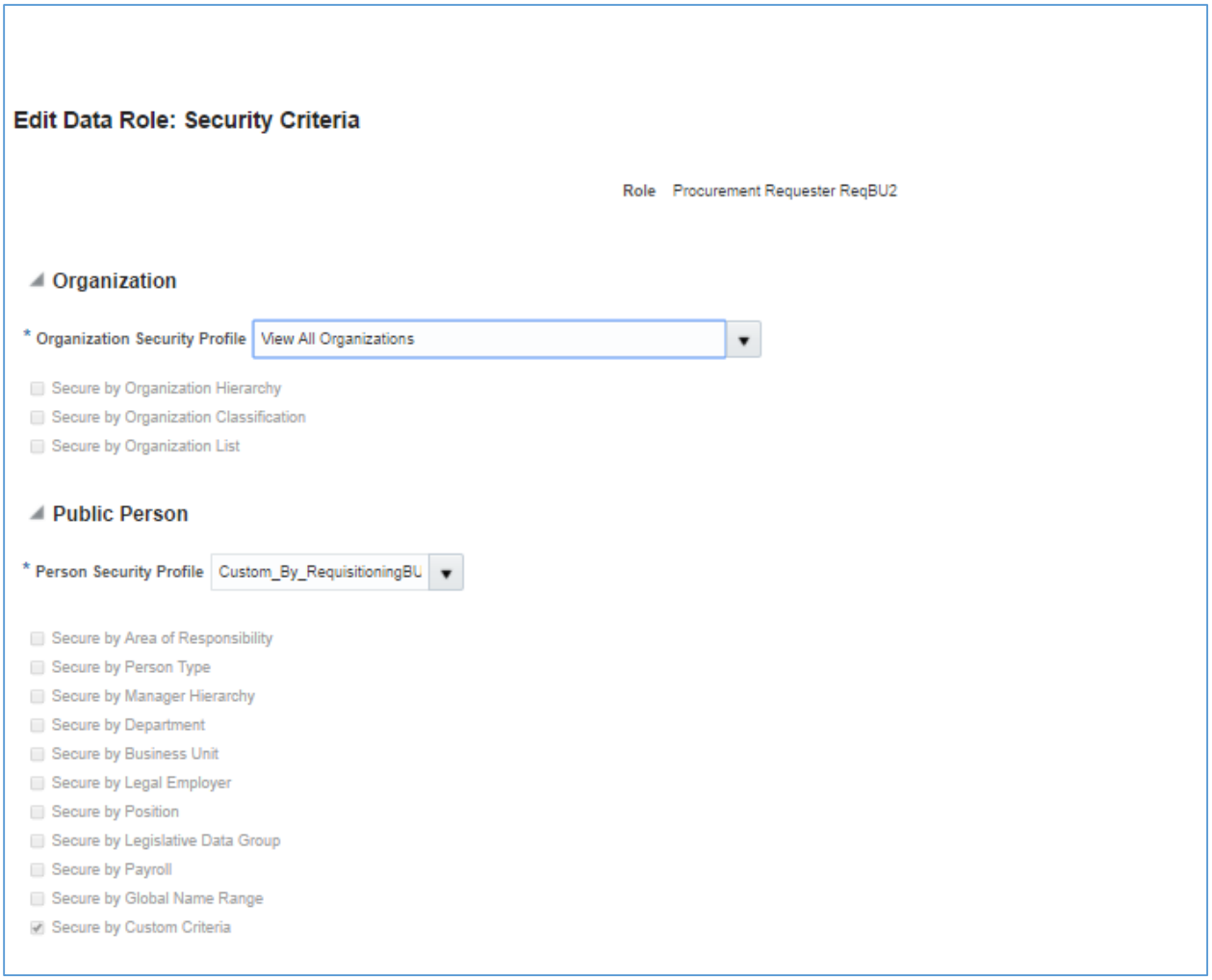
```
&TABLE_ALIAS.PERSON_ID IN
(
   SELECT PERSON_ID FROM PER_ALL_ASSIGNMENTS_M WHERE BUSINESS_UNIT_ID IN
    ( SELECT business_unit_id FROM per_all_assignments_m AM
       WHERE AM.person_id =(SELECT HRC_SESSION_UTIL.GET_USER_PERSONID FROM DUAL)
       AND trunc(sysdate) between AM.effective_start_date and AM.effective_end_date
       AND AM.EFFECTIVE_LATEST_CHANGE='Y' AND AM.PRIMARY_FLAG='Y'
       AND AM.ASSIGNMENT_STATUS_TYPE IN ('ACTIVE', 'SUSPENDED') )
   AND trunc(sysdate) between effective_start_date and effective_end_date

    AND EFFECTIVE_LATEST_CHANGE='Y'
   AND PRIMARY_FLAG='Y' AND ASSIGNMENT_STATUS_TYPE IN ('ACTIVE', 'SUSPENDED')
   )
```

Step 3: Assign the custom person security profile to the newly created Procurement Requester and Employee Roles

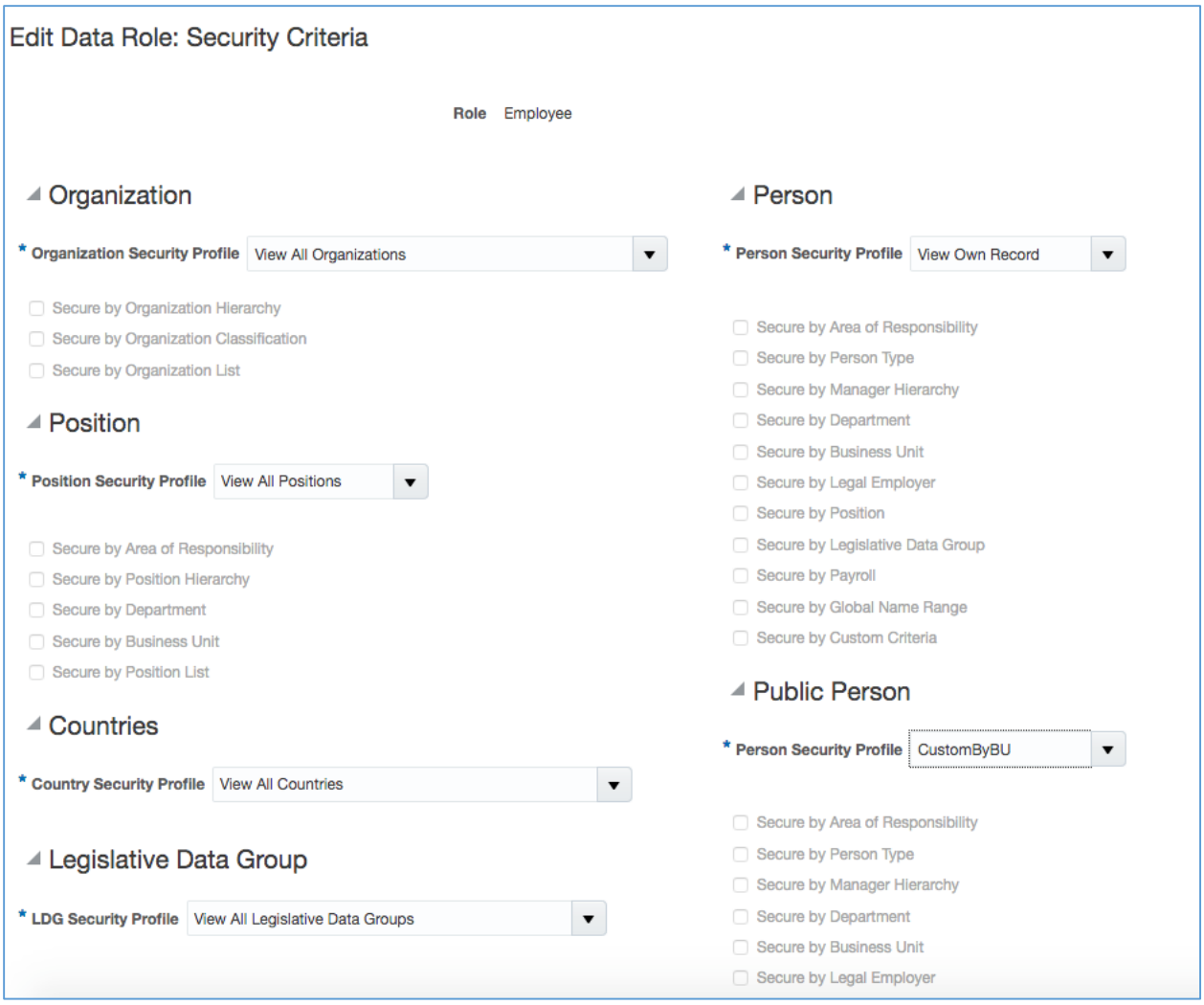
A) For the Requester role

Setup and Maintenance > Manage Data Role and Security Profiles > Person Security Profile > <NEW_PERSON_SECURITY_PROFILE>



B) For the Employee role

Setup and Maintenance > Manage Data Role and Security Profiles > Public Person > <NEW_PERSON_SECURITY_PROFILE>

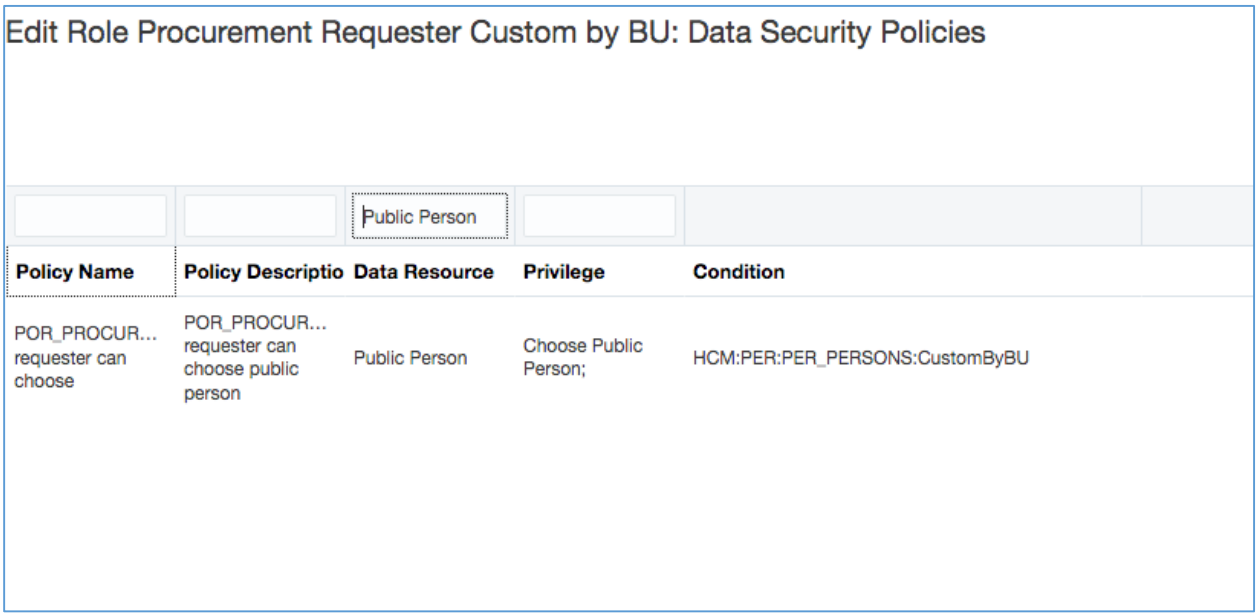

Edit Data Role: Security Criteria
Role Employee
Organization
* Organization Security Profile View All Organizations
Secure by Organization Hierarchy
Secure by Organization Classification
Secure by Organization List
Position
* Position Security Profile View All Positions
Secure by Area of Responsibility
Secure by Position Hierarchy
Secure by Department
Secure by Business Unit
Secure by Position List
Countries
* Country Security Profile View All Countries
Legislative Data Group
* LDG Security Profile View All Legislative Data Groups
Person
* Person Security Profile View Own Record
Secure by Area of Responsibility
Secure by Person Type
Secure by Manager Hierarchy
Secure by Department
Secure by Business Unit
Secure by Legal Employer
Secure by Position
Secure by Legislative Data Group
Secure by Payroll
Secure by Global Name Range
Secure by Custom Criteria
Public Person
* Person Security Profile CustomByBU
Secure by Area of Responsibility
Secure by Person Type
Secure by Manager Hierarchy
Secure by Department
Secure by Business Unit
Secure by Legal Employer

Step 4: Remove the seeded Data Security Policies (DSP) from the new Procurement Requester role *(this will leave just the new DSP we assigned to the role in Step 3)*

Security Console > [NEW_PROCUREMENT_REQUESTER_ROLE] > Edit Role> Data Security Policies

Filter by Data Resource = Public Person

You will see all DSPs assigned to Public Person including one bearing the name of the person security profile you created. Remove all the others

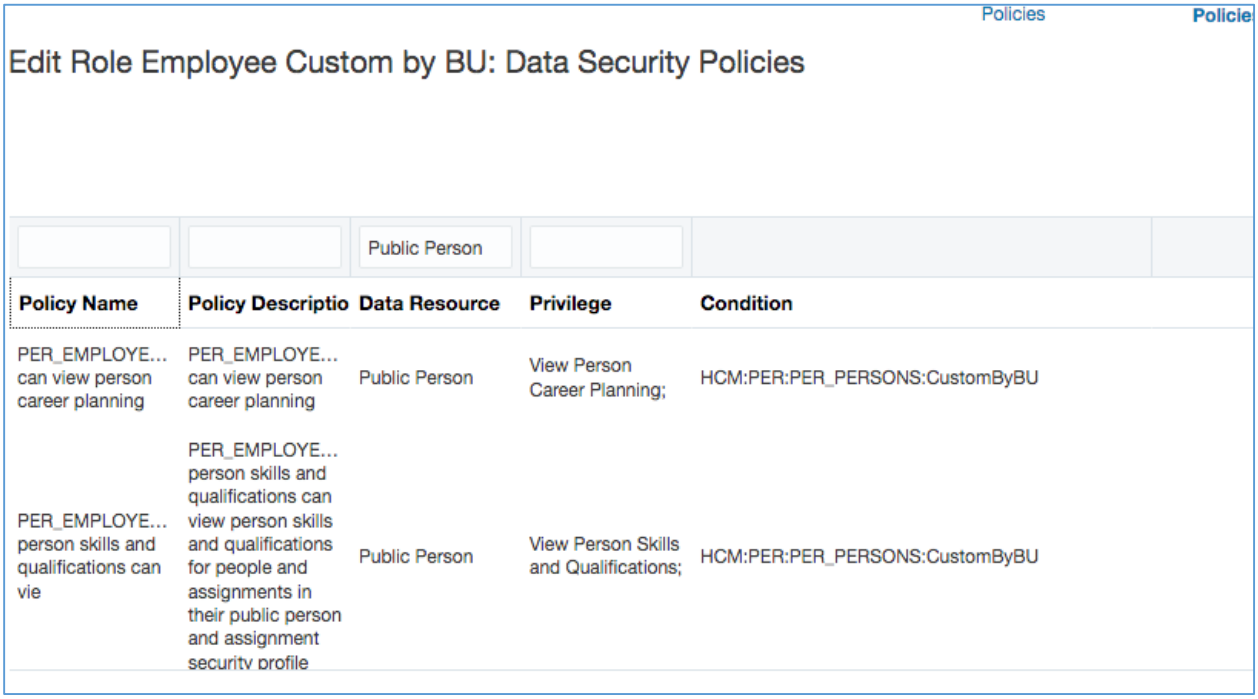

Edit Role Procurement Requester Custom by BU: Data Security Policies

		Public Person		
Policy Name	**Policy Descriptio**	**Data Resource**	**Privilege**	**Condition**
POR_PROCUR... requester can choose	POR_PROCUR... requester can choose public person	Public Person	Choose Public Person;	HCM:PER:PER_PERSONS:CustomByBU

Step 5: Remove the seeded DSPs from the new Employee role (leaving only the new DSP which you assigned in Step 3)

Security Console > [NEW_Employee_ROLE] > Edit Role> Data Security Policies

Filter by Data Resource = Public Person



Notes

a) Employee role has several DSP for the Public Person data resource
b) Each of the seeded ones have to be removed leaving only the ones from the new DSP assigned in step 3
c) One way to simplify this task is to filter by each value in the privilege column. This will give you the seeded rows and the newly assigned rows. You then delete the seeded rows. For example filter by 'View Person Career Planning', 'View Person Skills and Qualifications', etc

Step 6: Assign the new employee role to your users and remove the old employee role from them