Security Liaison Guide

This page intentionally left blank

Security Liaison Guide

Table Contents

Overview

HRMS & Financial Security Liaison Roles

The role of Security Liaison within an agency is critical to the continued success of the Core-CT application. Each Agency has one or more Security Liaisons for HRMS and Financials. The Security Liaison is the Security Team's point of contact at each agency for security related requests, issues, and communication. Security Liaisons are responsible for reviewing security requests and creating an online CO1092.

Depending upon whether the Security Liaison handles financial roles or human resources roles, the liaison will have the role of CT AGY FINANCIALS SEC LIAISON and/or CT AGY HRMS SECURITY LIAISON which provides read only access to the following:

- User Profiles - Navigation: *(Core-CT FIN, HRMS, or EPM) > PeopleTools > Security > User Profiles > User Profiles*. The General & Roles tabs in FIN, HRMS, EPM, and Portal are displayed. The General tab displays the User ID, description and email address link. The Roles tab displays the roles associated with the User ID.

- Roles – Navigation: *(Core-CT FIN, HRMS, or EPM) > PeopleTools > Security > Permissions & Roles > Roles.* The General & Members tabs in FIN, HRMS, EPM, and Portal are displayed. The General tab displays the role name and its description. The Members page displays a maximum of 1000 User IDs that have that role.

- Time & Labor Security Setup – Navigation: *Core-CT HRMS > Set Up HRMS > Security > Time and Labor Security > TL Permission List Security*. The Row Security Permission List tab displays Security information. The Row Security Users tab has been disabled.

- Time & Labor Permission Lists and Security by Department Tree – *Navigation: Core-CT HRMS > Set Up HRMS > Security > Core Row Level Security > Security by Dept Tree*. The Security by Dept Tree displays the Row Security Permission List and associated DeptID.

- Requester and Buyer Set Up – Navigation: *Core-CT Financials > Set Up Financials/Supply Chain> Product Related > Procurement Options > Purchasing > Buyer Setup or Requester Setup*. Buyer Setup displays Department, Ship To, Location (asset), and Origin. Requester Setup displays Ship To, Location (asset), Origin, and default Chartfields.

- User Preferences for Financials – Navigation: *Core-CT Financials > Set Up Financials/Supply Chain> Common Definitions > User Preferences > Define User Preferences.* From General Preferences, click Overall Preference for Business Unit and SetID information. Click any link in Product Preference to display User ID information about that module. If the User ID does not have access to that module the display will not change.

The listing of Security Liaisons can be found in two ways:

- In the application by navigating to *(Core-CT HRMS, Financials or EPM) > PeopleTools > Security > Permissions and Roles > Roles*, opening up CT AGY FINANCIALS SEC LIAISON or CT AGY HRMS SECURITY LIAISON, and clicking on the Members Tab.

- From the internet: Core-CT Home Page > Agency Security Liaison > Financials Agency Security Liaisons List **or** HRMS Agency Security Liaisons List

Password Reset Role

In accordance with OSC Memorandum 2014-10, September 22, 2014, Comptroller's Core-CT Systems Security for State Employees, the role of resetting passwords for users in Core-CT is now available for authorized Security Liaisons in state agencies. Moving this responsibility to the agencies will give the agency more control over user access issues as well as streamline the password reset process. A new menu item, Distributed User Profiles, has been added in Core-CT for this purpose.

A new role has been created to restrict access to resetting passwords and auditing User Emails and System Profiles. The role name is CT SECURITY LIAISON and can be found in both the Financial and HRMS role handbooks as of 12/15/11.

The Security Liaison role provides only access to the following:

- Distributed User Profiles – Navigation: *Main Menu > Peopletools > Security > User Profiles > Distributed User Profiles.* The General and Forgot Password tabs are displayed in Portal. The General tab displays the User ID, description, Account Lock, Change Password and Password Expired information and a link to the user email address. The Forgot Password tab displays if a user has set up a primary email address and challenge question in their System Profile *(this is required in order to use the Automate Forgot My Password feature).*

Note-As of June 2019 resetting passwords is a 2 step process. The password must be reset and saved, then it must be expired and saved.

Current Primary Security Liaisons are responsible for the authorization and dissemination of this role in their agencies and use the on-line CO-1092 process to request access. Users do not have to have the regular liaison role: CT AGY FINANCIALS SEC LIAISON or CT AGY HRMS SECURITY LIAISON in order to have the CT SECURITY LIAISON role for the password reset function. The primary liaison will need to authorize the role for anyone who is not a regular liaison.

The Liaison must also provide all relevant information and training to additional staff prior to assigning the role; the Core-CT Security team can be also be available to train, upon request.

For information on Password Reset Instructions, please navigate to Core-CT Security Website as follows: https://www.core-ct.state.ct.us/security/pdf/Liaison_password_reset9_2_051719.pdf

CO-1092 On-Line Security Request Creator Role

The CO-1092 HRMS and Financial Application Security Request forms have been automated, as of July, 2013. A new menu item, CO-1092 Security Request, has been added in Core-CT HRMS and Financials for this purpose.

As with the previous paper CO-1092 Forms, Security Liaisons should continue to work with unit supervisors to determine the role access the user should have. Existing or new Security Liaisons will require an additional role to be able to use the on-line CO-1092 Security Request Form.

A new role has been created to restrict access for creating CO1092 Security Requests on-line. The role name is CT_CO1092_LIAISON and can be found in both the Financial and HRMS Role Handbooks as of July 3, 2013.

The CO-1092 Liaison role provides only access to only the following:

- On-Line CO-1092 Security Request Form - Navigation: *Main Menu > Core-CT (HRMS or Financials) > PeopleTools > Security > CO-1092 Security Request*

  Find and Existing Value and Add New Values tabs are displayed in HRMS or Financials. Liaisons can search their existing requests by Transaction Number, Transaction Date, User ID, Employee ID, Name and/or Workflow Status. Liaisons can only see Transactions they have created or create new requests for employees they have access to and based on their row security in HRMS.

For guidelines on use of this role, please navigate to the Core-CT Security Website as follows: http://www.core-ct.state.ct.us/security/pdf/CO-1092_liaison_guide.pdf

CO-1092 On-line Approving Manager Role

The on-line CO-1092 HRMS and Financial Application Security Request process uses an on-line application workflow engine. Once a CO-1092 Liaison creates a Security Request on-line and submits for approval, a workflow process is triggered and the request is sent to the designated Approving Manager for review and approval.

A new role has been created to restrict access to designated Agency Approving Managers. The role name is CT_CO1092_APPRV_MGR and can be found in both the Financial and HRMS role handbooks as of July 3, 2013.

The CO-1092 Approving Manager Role provides access to only the following:

- CO-1092 Manager Approvals – Navigation*: Main Menu > Core-CT (HRMS or Financials) > PeopleTools > Security > CO-1092 Security > CO-1092 Manager Approvals*

  Find and Existing Value tab is displayed in HRMS or Financials. Approving managers can search their existing requests by Transaction Number, Transaction Date, User ID, Employee ID, Name and/or Workflow Status. Approving Managers can only see/approve Transactions that have been submitted to them for employees they have access to and based on their row security in HRMS.

Note: Additional CO-1092 Security Request Approver Roles exist to support OSC and DAS role approvers and the Core-CT Security Team Administrators in the CO-1092 Workflow, however, these are for Central Agency use only.

For guidelines on use of this role, please navigate to the Core-CT Security Website as follows: http://www.core-ct.state.ct.us/security/pdf/CO-1092_appr_mgr_guide.pdf

Understanding Core-CT Security

Within Core-CT, security is determined through Permissions Lists, Roles, and User Profiles.

Permission Lists basically control all security within Core-CT. Permission Lists are lists, or groups, or authorizations to which Roles are assigned. They determine what pages a user can see within the application, what data a user can see within these pages, and what actions (e.g., add, update, view) a user can take on the data. Permission Lists store such things as sign-on times, menu access, page access, and component access. Updates to a Permission List affect all the roles that contain that permission list. Data permissions are separate from page permissions.

Some permission lists may also be considered a role. The concept is called Role Layering, and it is used when one role is fundamental to another role (e.g., the PO Viewer role is a necessary part of the General Buyer role). Using this methodology maintains the concept of editing one Permission List (in this case, also a role) that is then applied to all roles that require the layered role.

Roles are intermediate objects that link Permission Lists and User Profiles. Roles are assigned to User Profiles. Multiple Permission Lists can be assigned to a single Role and multiple Roles can be assigned to a single User Profile. Some examples of Roles might be CT EMPLOYEE, CT GENERAL BUYER, CT AGY TIMEKEEPER, and CT AGY VENDOR VIEWER. Updates to a role affect all users that contain that role.

A User Profile is a set of data describing a particular user of the PeopleSoft system. User Profile data includes everything from language code, password, Business Unit, Workflow and Origins for PO & AP Transactions & Approvals, Department Security Tree, Location, email address to application-specific data that a user is authorized to access within the Core-CT application.

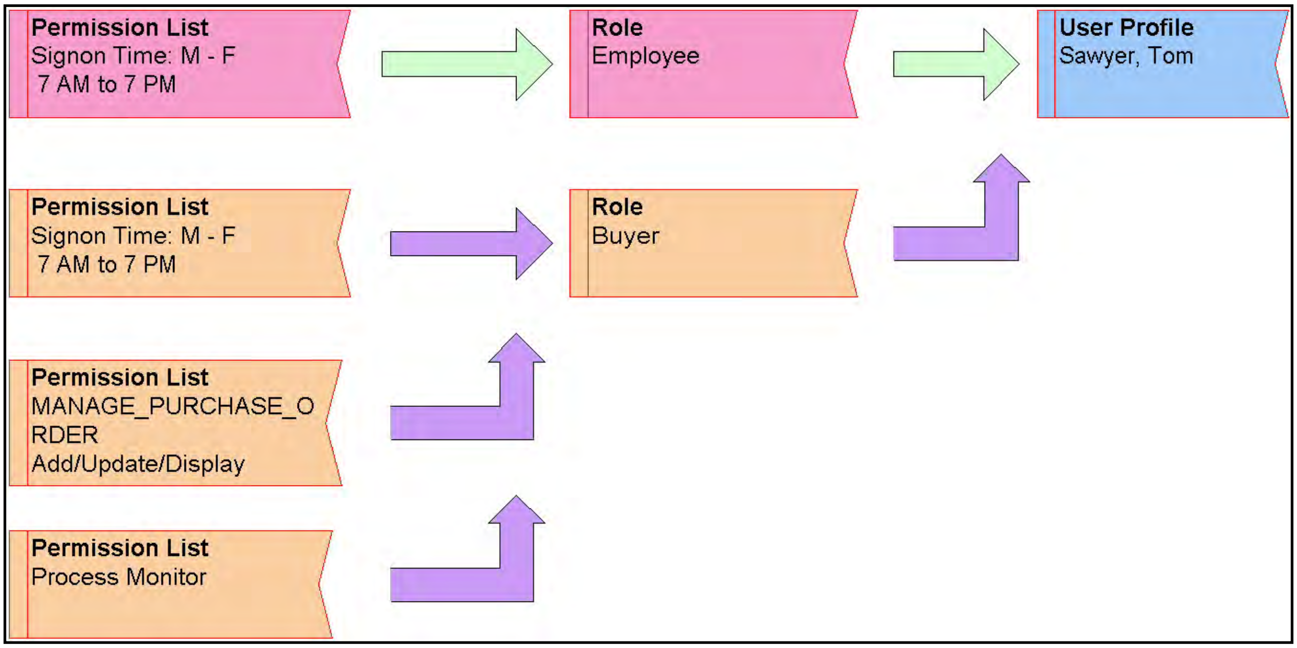

Figure 1 - An example of the hierarchical relationship between Permission Lists, Roles, and User Profiles.

Password Security Policies

The following password security policies are in effect:

- All passwords expire in ninety (90) days.
- Users will be warned for fifteen (15) days prior to the password expiration.
- Five (5) logon attempts are allowed before the account is locked out.
- The password cannot match the User ID.
- The password must be at least eight (8) characters in length, three (3) of which must be digits. Six (6) passwords are retained in the system.
- Both alphabetic and numerical characters are allowed.
- Passwords should be obscure rather than obvious.
- All users with valid email addresses must set up their user profile in Core-CT to be able to use the password reset feature in Core-CT. Please use the following link for instructions on setting up user profile: http://www.core-ct.state.ct.us/security/pps/pwreset.pps
- Only authorized agency security liaisons can request password resets from a Core-CT Application Security Administrator, when necessary.
- Effective November, 2011, primary Agency Security Liaisons will have the ability to reset passwords in their agencies.

Distribution of the User-IDs and passwords should be hand delivered or emailed by the agency security liaison. Agency personnel should be informed of the password guidelines and policies, procedures for password and access problems, and who to contact. Any problems associated with User ID's or passwords must be communicated through the Agency Security Liaison. Agency personnel are not to contact the Core-CT Security Administration directly.

Agency Liaison Responsibilities

Each agency has the responsibility to assign a Core-CT Security Liaison to be the primary contact for the Statewide Core-CT Applications Security Administrator. The Security Liaison is responsible for monitoring all authorized access to the Core-CT Financials/HRMS application to their agency personnel, and acting as point of contact for the Core-CT Applications Security Administrator. Each agency should develop internal security procedures for Financial, HRMS and EPM users.

The HRMS / Financials Security liaison's tasks include:

- Requesting new access for system users and changes to existing access.
- When an employee transfers from one agency to another, the employee's ID is reusable but Core-CT access has to be re-defined by the new agency.
- Maintaining confidentiality of User-ID's and passwords.
- Resetting User passwords when necessary and ensuring system profiles are set up and include valid email accounts.
- Submitting all new, change, or delete requests using the on-line CO-1092, Agency Application Security Request Forms.
- Liaison may share these responsibilities and tasks only with other authorized liaisons within the agency. **Core-CT Security Administration will not communicate security information to unauthorized agency personnel.**
- Contacting Core-CT Application Security Administrator with any questions regarding User-ID's, passwords or access.
- Retain the original CO-1092 (Core-CT Application Security Request Form) at the agency for auditing purposes (Paper forms only).

Password Reset Liaison tasks include:

- Resetting passwords in Core-CT for valid users and securely notify users of temporary passwords
- Locking out user account access immediately upon the notice of an employee’s termination, retirement, transfer to another department/agency
- Enforcing users to set up their system profile in order to utilize the automated password reset feature
- Updating user email addresses if incorrect or missing
- Contacting Core-CT’s Application Security Team with any questions and/or problems regarding user ids, passwords or access (NOTE: You may email a request for password resets to corect.security@ct.gov. Please do not contact the Help Desk.)
- Maintaining confidentiality of user id’s and passwords
- Enforcing that user id’s and passwords are not shared, attached to terminals, desk tops, or located where accessible to unauthorized personnel

- Enforcing that passwords are changed immediately if the employee suspects that the security of his or her password has been breached

It is each agency's responsibility to monitor the following:

- Review each user's access and restrict that access where the access is incompatible with the user's job description and/or does not provide proper segregation of duties. Approve only the employees required to perform the business functions.
- Enforce that User-ID's and passwords are not shared for convenience between personnel.
- Enforce that User System Profiles are set up to leverage the automated password reset process and include valid email accounts.
- Enforce that User-ID's and passwords are not attached to terminals, desktops, or located where accessible to unauthorized personnel.
- Enforce that passwords are changed immediately if the employee suspects that the security of his/her password has been breached.
- Correct user access when an employee has a change in responsibility within the agency.

Agency HR Security Responsibilities

The agency's human resource office must provide notification to the liaison of an employee's termination, retirement or transfer to another department/agency and the request for deletion of access on the date of separation will be made by the liaison. When an employee transfers from one agency to another, the employee's ID is reusable but Core-CT access has to be re-defined by the new agency. Agencies should consider employing an employee exit checklist to ensure that employees who are leaving an agency have their user ID disabled.

Employee supervisors should review each user's access and restrict that access where the access is incompatible with the user's job responsibilities and/or does not provide proper segregation of duties. They should ensure that users only have the roles they need to perform their business functions. User-IDs and passwords are not shared for convenience between personnel. User-IDs and passwords are not attached to computers, desks tops, or located where accessible to unauthorized personnel.

Where it is necessary for a user to be assigned roles that do not allow for the proper segregation of duties, supervisors will be required to provide documentation to Core-CT (via their Security Liaison) that explains why the roles are necessary within the agency and describe the audit functions in place to prevent inappropriate actions being made by a user (e.g., hiring a fictional employee and then paying them). .

Passwords should be changed immediately if the employee suspects that the security of his/her password has been breached.

Role access to should be reviewed when an employee's job duties change.

The agency is responsible to perform a quarterly audit of agency users to identify terminated employees who still have active user IDs. Agency Liaisons will run EPM Reports to verify status of roles assigned to User Profiles. The agency may want to have someone other than the Security Liaison perform this task.

CO-1092 Process / Responsibilities

First and foremost, Primary Agency Liaisons should ensure any Security Liaisons, Password Reset Liaisons and Approving Managers are properly trained and in place in their agency. For end users, Liaisons work with the unit supervisor to determine the role access the user should have. Employees may perform one or more roles, based on your agency's organizational structure. In addition, more than one employee may perform a role within your agency. In determining the role access, the security liaison and the unit supervisor should be aware of separation of duties issues.

The Security Liaison and Managers should be acquainted with the roles in the role handbook. The Help Desk is prepared to answer questions about specific roles.

The retention period for the CO-1092 is two years from the date that an employee separates from an agency. The original copy (paper forms) is retained by the submitting agency. Destruction can occur after the minimum retention period and submission to the State Library for approval of the form RC-108: http://www.cslib.org/publicrecords/Forms/RC108rev201107.doc
Security Liaisons will not need to create or retain paper versions of the newer CO-1092 electronic forms for retention purposes; electronic Forms are stored (indefinitely) in database tables in Core-CT for accessible for auditing at any time.

Completing the CO-1092

Overview

Security in the Core-CT system is imperative and only those individuals authorized should have access. Non-State employees cannot have access to the Core-CT System.

Each agency has the responsibility to assign a Core-CT Security Liaison to be the primary contact with the Statewide Core-CT Applications Security Administer. The Security Liaison is responsible for monitoring all authorized access to the Core-CT Financials/HRMS application to their agency personnel and acting as point of contact for the Core-CT Applications Security Administrator.

Certain roles highlighted in Bold and starting with a double asterisk (**) require additional information that can be provided on the Financials Appendix – Required Additional Role Information.

The Security Team grants a two (2) week window for processing CO-1092 requests; Liaisons may contact the Security Team for form status after a 2 week period has passed.

Security Request Form (CO-1092)

Retention Period – Paper CO-1092 Forms Only (before July, 2013)

The Connecticut State Library with the Office of the State Comptroller has determined that agencies shall retain the original documents for "two (2) years from employee's separation of service."

The State Library is in the process of revising the S3: Fiscal Records schedule which will include this form. You may not destroy these records until the State Library issues the revised schedule. Please note that no public record may be destroyed until receiving a signed Records Disposal Authorization (Form RC-108) from the State Library.

CO-1092 – Automated Application Security Request Forms (eff. July, 2013)

Please refer to the CO1092 Completion Guidelines link below which will explain how to fill out an online HR or Financials Security requests:

http://www.core-ct.state.ct.us/security/hrms_sec.html

http://www.core-ct.state.ct.us/security/fin_sec.html

CO-1092 Tips for Financial Security Liaisons

Requisition Related Tips

- For a user assigned the role of *Requester*, a **Location, Department Number,** and **PO Origin** must be identified.
    - Only one Location and PO Origin may be assigned to a user
- For a user assigned to Requisition-related roles (see below), the **Requesters for which the user is authorized to perform actions** must be identified
    - The Requisition-related roles are:

        CT REQUESTER
        CT DELETE REQUISITIONER
        CT PSA_POS REQUESTER
        CT WF REQ AMT APPROVER 2
        CT WF REQ AMT APPROVER 4
        CT WF REQ PURCH APPROVER
        CT CANCEL REQUISITIONER
        CT REQUISITION CLOSER
        CT WF REQ AMT APPROVER 1
        CT WF REQ AMT APPROVER 3
        CT WF REQ BUDGET APPROVER
        CTMULTIREQUESTER

  - Example #1: if a user is a Requisition Closer, the user will be able to close requisitions ONLY for those Requesters identified.
  - Example #2: if a user is a Requester and creates requisitions on behalf of other Requesters, then those Requesters must specifically be listed.
  - *** **DEFAULTS** will be set up as follows:
    - Requesters will be authorized for themselves
    - All other roles above will be authorized for ALL Requesters (within the same Business Unit)

- For a user assigned to Requisition-related Approval roles, the **PO Origin(s) and Business Unit(s) for which the user is authorized to approve** must be identified
  - These Approval roles are:

    CT WF REQ AMT APPROVER 1
    CT WF REQ AMT APPROVER 2
    CT WF REQ AMT APPROVER 3
    CT WF REQ AMT APPROVER 4
    CT WF REQ BUDGET APPROVER
    CT WF REQ PURCH APPROVER
    CT AGY SERVICE APPROVER
    CT_F_A_PSA_POS_SUBMITTER

  - Multiple PO Origins can be entered

Purchasing Related Tips

- For a user assigned the role of *Buyer*, a **Ship To Location, PO Origin, and Department** must be identified.
  - Only one Ship To Location, PO Origin, and Department may be assigned to a user
  - If a user also has the role of Requester, the same Location and PO Origin may be used

- For a user assigned to Purchasing-related roles, the **Buyers for which the user is authorized to perform actions** must be identified
  - The Purchasing-related roles are:

    CT GENERAL BUYER
    CT PURCHASE ORDER CLOSER
    CT CANCEL PURCHASE ORDERS
    CT PROGRAM BUYER

  - Example #1: if a user is a Cancel Buyer, the user will be able to cancel purchase orders ONLY for those Buyers identified.
  - *** **DEFAULTS** will be set up as follows:
    - Buyers will be authorized for themselves
    - All other roles above will be authorized for ALL Buyers (within the same Business Unit)
- For a user assigned to Purchasing/Requisition-related Approval roles, the **PO Origin(s) and Business Unit(s) for which the user is authorized to approve** must be identified
  - These Approval roles are:

    PO Amount Reviewer 1
    PO Amount Approver 2
    PO Budget Reviewer

- Multiple PO Origins can be entered

Voucher Related Tips

- For a user assigned the role of *Voucher Processor*, an **AP Origin** must be identified.
  - Only one AP Origin may be assigned to a user
- For a user assigned the role of *Voucher Approver* or *Alternate Approver*, the A**P Origin(s) and Business Unit(s) for which the user is authorized to approve** must be identified.
  - Multiple AP Origins can be entered

Claims Authorization Form (CO-512)

Form CO-512 is available for downloading from the Office of the Comptroller's website at http://www.osc.ct.gov/agencies/forms/index.html. The original hard-copy form must be completed and forwarded to the Comptroller's Office, Accounts Payable Division, 55 Elm Street, Hartford, CT 06106 Attention: Linda Arn.

The CO-512 must contain the names of all agency personnel with the final approver role(s) listed below.

Name Changes

If the name of a final approver changes then a new CO-512 needs to be submitted since the information on the CO-512 will not match the user profile.

Final Approver Roles:

- Requisition Purchasing Approver
- Purchase Order Budget Reviewer/Approver
- Voucher Approver
- Alternate Approver

The 'new' box on the CO-512 form should only be checked off at the beginning of each fiscal year. Any changes thereafter should have the 'update' box checked.

Name Changes:

Any user, who has final approval roles and requests a name change, will need to ‘update’ the CO-512 to reflect the new name.

When submitting an ‘updated’ CO-512 form, all final approvers must be listed. This updated form will supersede all previously submitted forms. Therefore, all employees with final approver roles must be listed on the updated form.

Please refer to the State of CT Comptroller website for additional info regarding the CO-512.

Secondary User IDs

The standard reasons to be given a secondary User ID are Interface IDs which start with IR prefix, dual employment, 1099 processing (OSC), DOT 24/7 seasonal IDs. Once the approval for a secondary id has been granted:

- Liaison will send an email to corect.security@ct.gov requesting that a secondary **ID** be created. The liaison will provide the name and employee number.
- The security team will create an **ID** for the user with a number 2 suffix (ex: if the current userid is SmithR, it will be SmithR2)
- If, however, the current **ID** for the user is a numeric **ID** (ex: 001234) then an alpha user**ID** will need to be created based on the user's last name and first initial(s).
- The security team will email the user**ID** to the liaison.
- The liaison will now be able to select the secondary user **ID** in order to create an online CO-1092 request.

Financial Security

The Financial Role Handbook

Role descriptions are a summary of the individual tasks outlined in each business process. The role descriptions in the handbook identify the major tasks assigned to the role from an agency's perspective, as well as the interactions with other roles that are critical to completing a business process.

An analysis of these roles was made to determine whether the tasks are performed by Central or Line Agency. This handbook covers both Line Agency and Central Agency Roles.

Origins

Origin code values are the basis of workflow routing rules since they can be defined to represent different approval levels. In Core-CT origin codes are used to identify the department, or group (agency, bureau, division, unit) within an agency, from which transactions originate. Origin codes facilitate the grouping of transactions, allow an additional level from which information can default into transactions, and provide a more detailed level of reporting within an agency.

Origins are three character representations of an Agency, Bureau, Division or Unit. Agencies determine the level that is represented. Agencies submitting requests for new Origins do not get to select the 3 character values. They are assigned randomly by Core-CT based on availability.

Origins and Workflow

As stated above, Origins are used to identify where transactions Originate. This identification is also used in workflow. Simplistically, users who have been given the role of approver (ePro, Purchasing, or Accounts Payable) have also been assigned Origins for which they can approve. Where the transaction Origin (i.e., the transaction Originator) is the same as the Origin assigned to the approver then that approver will be able to see and approve that transaction. Where they are different then the approver will not be able to see the transaction.

Terminology

Workflow – Automated method for routing of transactions (requisitions, purchase orders, vouchers) for approvals.
User – Single person set up in the PeopleSoft system.
Location – An address in the system where items can be shipped to or invoiced to.
Role – High level definition of permissions assigned to groups of users. A User may have multiple roles.
Routing – Method by which transactions flow through the approval chain.
Module Business Unit – PeopleSoft method for separating transactions based on business rules for AP, PO and AR.
Origin – Identifies agency's origination of a transaction and is means to route transactions for approvals.
Requester – User who enters requisitions into PeopleSoft.
Buyer – User that will be final approver of requisitions and creates purchase orders.
Approver – User assigned specific approval limits in each module.

Assignment of One Origin for Transactions

When assigning an individual to the Role of Requester, Buyer, Voucher Processor, or Voucher Build Processor, you must assign ONE and ONLY ONE Origin for transactions for each Role. Some agencies have identified issues with the assignment of only one origin, specifically in the case of Buyers and Requesters. The issue involves situations where a Buyer or Requester wants a Purchase Order or Requisition to route to a specific Approver depending upon the type of PO or Requisition or the Funds used to pay for the PO or Req. For example, there may be separate approvers for General Fund purchases and Bond Fund purchases, but one Requester or Buyer can generate transactions against both types of funds.

Open a Help Desk ticket through FootPrints if you run into such a problem. The appropriate Core-CT staff will discuss the options available to you.

Segregation of Duties for Origins and Workflow

It is important when assigning roles that agencies pay attention to Segregation of Duties guidelines, specifically the following:

1. A User should not be able to create a Purchase Order and approve it without any other User being involved in the process.
   - No Buyer will have all 3 Approval Roles (Amount 1, Amount 2 and Budget).
   - A Buyer who has either of the Amount Approval Roles will not have the Budget Approval Role and, conversely, a Buyer who has the Budget Approval Role will not have either of the Amount Approval Roles.
   - Users with a Role of Buyer and any of the Approval Roles will have different origins for their Buying Source Origin and their Approval Origin.
2. A user with either PO Amount Approver Role or Budget Approver Role should not also have Voucher Approver role.
3. A User should not be able to create a Requisition and approve it without any other User being involved in the process.
   - No Requester will have all 6 Approval Roles (Amount 1, Amount 2, Amount 3, Amount 4, Budget, and Purchasing).
   - A Requester who has any of the Amount Approval Roles will not have the Budget Approval Role and, conversely, a Requester who has the Budget Approval Role will not have any of the Amount Approval Roles.
   - Users with a Role of Requester and any of the Approval Roles will have different origins for their Buying Source Origin and their Approval Origin.
4. A User should not be able to create a Voucher and approve it without any other User being involved in the process.
   - A Voucher Processor should not also have the Role of Voucher Approver

Tips & Guidelines for Mapping Users & Roles

A. General Tips & Guidelines

- Core-CT roles are designed to provide flexibility. Agencies decide how many and what roles each user should have;
- Users may have responsibilities that are cross-modular. If applicable, consider roles in all module areas. For example, it is likely that AP personnel will need access to purchasing information;

contract personnel may need access to all financial areas; Accounts Receivable staff may need access to the General Ledger, etc.

- Consider Report Maker or Viewer roles to supplement a user's main processing role.

B. Notes about Specific Roles

- The following roles should be assigned to very few people:

  CT WF REQ AMT APPROVER 3, 4
  CT WF REQ BUDGET APPROVER,
  PO Budget Reviewer
  CT PURCHASING ERROR PROCESSOR
  CT CONTRACT HOLDER
  CT CONTRACT CLOSER
  CT SPEEDCHART MAINTAINER
  CT INTERFACE USER
  CT PURCHASE ORDER CLOSER
  CT ADJ VOUCHER PROCESSOR
  (reversal vouchers also)
  CT VOUCHER BUILD PROCESSOR
  CT BUDGET CHECK PROCESSOR
  CT VOUCHER MAINTENANCE PRCSR
  Alternate Approver
  CT INTRFACE ERR HDLR DRS/TREAS

- Roles are created that may appear to have similar access (e.g.: Delete/ Cancel Buyer, Contract Holder, Contract Creator). As an example, the Cancel Requester is responsible for canceling reqs, while a Delete Requester is responsible for deleting reqs. These types of roles are created to provide distinct access, if your agency requires it.

Purchasing

- A Casual Receiver role can only receive against requisitions they created. So, there should be a one-to-one correspondence between the Requester role and the Casual Receiver role.
- Requisition workflow is separate and distinct from Purchase Order workflow. If a person performs both duties, they need both types of roles.
- A General Buyer is usually the final approver in the Requisition approval process, but in the Requisition workflow, the role needed is Requisition Purchasing Approver. Therefore a user needs the Requisition Purchasing Approver role for the Requisition workflow and the General Buyer role for the Purchase Order Workflow.
- A General Buyer often performs duties related to Contracts, PO's, and Requisitions. Therefore, a user with the General Buyer role may also need access to these additional roles:

  CT CANCEL REQUISITIONER
  CT REQUISITION CLOSER
  CT CONTRACT CREATOR
  CT CONTRACT CLOSER
  CT DELETE REQUISITIONER
  CT CONTRACT APPROVER
  CT CONTRACT HOLDER

- A user must be assigned the role of Buyer if the user is assigned any of the following roles:

  CT CANCEL PURCHASE ORDERS
  CT GENERAL BUYER
  CT PURCHASE ORDER CLOSER
  CT PROGRAM BUYER
  CT PURCHASING ERROR PROCESSOR

- A user must be assigned the role of Requester if the user is assigned any of the following roles:

  CT CANCEL REQUISITIONER
  CT DELETE REQUISITIONER
  CT REQUISITION CLOSER

Accounts Payable

- A Voucher Approver is included in the workflow setup. An Alternate Approver is not included in workflow and will have to navigate in Core-CT to his or her Worklist page to approve a voucher.
- Budget Check Processor should also be assigned Voucher Viewer and Purchase Order Viewer.
- A user assigned to the Voucher Processor or Template Voucher Processor role also should have the role of Agency Vendor Processor.
- A user assigned to the Voucher Approver, Alternate Approver, AP Reviewer, or Budget Check Processor role also should have the role of Voucher Viewer.
- A user assigned to the Journal Voucher Processor, AP Reviewer, and Central AP Viewer role also should have the role of Vendor Viewer.

Accounts Receivable

- A Billing Processor should not be an Accounts Receivable Processor, and vice versa.

General Ledger

- If a GL user needs to see details about specific transactions ("drill-down" capability), then the user should be assigned the appropriate viewer roles for the other modules (e.g., AP Viewer, Requisition Viewer, Receivable Viewer)

Inventory

- The Agency Inventory Processor cannot have any other Inventory role except the Agency Inventory Reviewer role.
- The Agency Inventory MSR Creator cannot have any other Inventory role except the Agency Inventory Reviewer role. The Agency Inventory MSR Creator can have the role of Agency Inventory Express Issuer if the User is from a DOT Repair Shop.
- The Agency Inventory Express Issuer cannot have any other Inventory role except the Agency Inventory Reviewer role. The Agency Inventory Express Issuer can have the role of Agency Inventory MSR Creator if the User is from a DOT Repair Shop.
- The Agency Inventory MSR Approver cannot have any other Inventory role except the Agency Inventory Reviewer and Agency Inventory Financial Processor roles.
- The Agency Inventory MSR Processor cannot have any other Inventory role except the Agency Inventory Reviewer and Agency Inventory MSR Approver roles.
- The Agency Inventory Adjuster cannot have any other Inventory role except the Agency Inventory Reviewer and Agency Inventory Financial Processor roles.
- It is recommended that the Agency Inventory Review role be given to all Inventory users.
- The Agency Financial Inventory Processor role can have the Agency Inventory MSR Approver, Agency Inventory Adjuster and Agency Inventory Reviewer roles. However, the Agency Inventory MSR Approver and Agency Inventory Adjuster roles can never be combined.

Asset Management

- A General Buyer and General Receiver cannot have the roles of Agency Asset Processor or Agency Financial Asset Processor.
- A Voucher Approver cannot have the roles of Agency Asset Processor or Agency Financial Asset Processor.
- Asset roles can also receive against a purchase order.
- Asset roles may also update a purchase order
- An Asset Processor should not be able to approve a purchase order.
- An Asset Processor should not be able to approve a voucher.

HRMS Security

The HRMS Role Handbook

The handbook describes Core-CT HRMS Roles. These roles are cross-agency or function specific. The handbook is intended to aid agencies in the process of mapping personnel to Core-CT roles. Multiple roles may, and in many cases, should be assigned to an individual employee. Roles are not intended to reflect job titles, current or future!

Each agency needs to understand how their business processes operate and what skills are necessary to perform these functions.

Role descriptions are a summary of the individual tasks outlined in each business process. The role descriptions in the handbook identify the major tasks assigned to the role from an agency's perspective, as well as the interactions with other roles that are critical to completing a business process.

An analysis of these roles was made to determine whether the tasks are performed by Central or Line Agency. This handbook covers both Line Agency and Central Agency Roles.

HRMS Security Guidelines

In an effort to maintain a segregation of duties between the HRMS responsibilities, agencies should not be requesting the Agency HR Specialist role be assigned to an employee who has either the Agency Payroll Specialist or Agency Time and Labor Specialist roles. Access to any combination of those roles could allow an individual to hire and pay someone inappropriately and without oversight. (see the Descriptions of Specific HR Roles section below).

Agencies that currently have employees with those combinations of roles will be contacted by the HRMS team to determine which Specialist roles are appropriate for the employee and where the viewer roles should be used.

For those agencies that currently have employees with these combinations of roles, or for future security requests where an agency feels it has a compelling need to have one individual maintain a combination of these roles, agency Security Liaisons must provide supporting documentation to explain the necessity of the dual roles, as well as explaining what their internal audit procedures are to prevent inappropriate or fraudulent transactions in the system.

Impacts from the 9.1 Upgrade

In conjunction with new Self-Service functionality being deployed with the 9.1 Upgrade in October 2012, changes to security processing occurred. The following summarizes these security-related changes that Security Liaisons need to be aware of with this system wide upgrade:

Current Core-CT Functional (HRMS, Financials, EPM) users will gain access to new Self-Service applications (eApps) in Core-CT to update personal information as well as view their paychecks on-line

- The creation of all brand new User IDs in Core-CT will be automated

- Moving forward, Employee ID (Emplid) will be used for all brand new User IDs

- Emplid will not replace existing (non-Emplid) User IDs

- Moving forward, Emplid will replace (non-Emplid) User IDs for name changes

- Security Liaisons will not be responsible for requesting the following self-service roles for Users in Core-CT: *CT AGY TL TIME REPORTER, CT EMPLOYEE and CT_H_U_EPAY.*

- Security Liaisons will discontinue the use CO-1092 Forms to create User IDs in Core-CT; User IDs will be created dynamically in the system upon hire of an employee.   The new employee's User ID will be their Employee; the new User ID's temporary password will be the first four (4) characters of the employee's last name plus the last four (4) digits of their SSN.

- Security Liaisons will continue to lockout Functional Users when terminated.

2) Agency Liaison Readiness Tasks

As a 9.1 Upgrade readiness task, Security Liaisons should ensure they have sufficient coverage to reset passwords for users in their agencies. The role CT SECURITY LIAISON, grants liaisons the ability to reset passwords, lock out user accounts, update email addresses and monitor system profile setup. This role can be requested on both the HRMS and Financials CO-1092 Application Security Request forms. Instructions on use of the User Distributed Profile Page in Core-CT as well as review of Password Controls and Policies will be provided upon assignment of the CT SECURITY LIAISON role. For more information on this role and password control policies, please refer to the following link on the Core-CT Security Website:

http://www.core-ct.state.ct.us/security/proc_updates.html

Tips & Guidelines for HRMS Mapping Users & Roles

General Tips & Guidelines

- Core-CT roles are designed to provide flexibility. Agencies should decide how many and what roles each user should have.
- Users may have responsibilities that are cross-modular in HRMS. If applicable, consider roles in all module areas. Example: Agency Benefit Specialist, Agency Time and Labor Specialist and Agency Payroll Specialist may all be the same employee at smaller agencies. However, do not assign an employee functional access to all four modules. Specifically, Core-CT will not approve both the Agency HR Specialist and the Agency Payroll Specialist for the same individual without documentation from the agency that explains why the roles are necessary and describing the audit functions in place to prevent inappropriate transactions by users. Consider the viewer roles in this case.
- Consider Report Maker or Viewer roles to supplement a user's main processing role.
- **Notes about** Roles are not intended to reflect job titles, current or future.

Descriptions of Specific HR Roles

Positions

- An Agency HR - Position Specialist has the ability to establish new positions and change characteristics of existing positions. (Traditionally, this role is assigned to Human Resources employees.) If the position enters workflow, it gets forwarded to the Agency HR – Personnel Administrator, Position Approver for approval.
- An Agency HR – Specialist administers the agency human resources process. In an effort to maintain a segregation of duties between the HRMS responsibilities, agencies should not be requesting the Agency HR Specialist role be assigned to an employee with either the Agency Payroll Specialist or Agency Time and Labor Specialist roles. Access to any combination of those roles could allow an individual to hire and pay someone inappropriately and without oversight.
- An Agency HR – Personnel Administrator, Position Approver also has the ability to establish new positions and change characteristics of existing positions. (Traditionally, this role is assigned to Personnel Administrators of the Agency.) If the position enters workflow, it gets forwarded to the Agency HR – Budget Specialist, Position Approver for approval. It also is the approver for positions that have entered workflow by the Agency HR – Position Specialist.
- An Agency HR – Budget Specialist, Position Approver also has the ability to establish new positions and change characteristics of existing positions. (Traditionally, this role is assigned to financial employees of the Agency.) If the position enters workflow, it gets forwarded to a Central Position Approver (either DAS or OPM or both) for approval. It also is the approver for positions that have entered workflow by the Agency HR – Position Specialist and/or Agency HR – Personnel Administrator.
- An Agency HR – Configuration Positions Specialist Judicial is only given to a small amount of Judicial employees in their HR department. This role maintains Judicial job code and Department ID combinations that do not require approval.
- An Agency HR – Positions Viewer only has access to view position data.

Employee Job Data

- An Agency HR – Specialist has the ability to hire or change employee information. Access to this role will allow updates to all modules located in Workforce Administration.
- An Agency HR – Viewer has the ability to only view employee information.

Workers Compensation

- An Agency HR – Workers' Compensation Specialist has the ability to process workers compensation transactions. This role has access to add or change Health and Safety, Job Data, Time Reporter Data and OSHA modules.
- An Agency HR – Workers' Compensation Viewer has the ability to view workers compensation transactions.

Job Code

- In order to view job codes, a user must have the role of Agency HR – Job Code Viewer.

HR Regulatory Specialist

- Agency HR – Regulatory Requirements Specialist is responsible for administering regulatory requirements. This role has access to the Disabilities module and has the ability to maintain data needed to substantiate that the State of Connecticut does not have discriminatory practices against people with disabilities.

- Agency HR – Regulatory Requirements Viewer is also responsible for administering regulatory requirements but only has access to view the data.

Recruitment Roles

- Currently the recruitment functionality has not been activated, therefore the roles of Agency HR - Hiring Manager and Recruitment Specialist do not provide additional access.

HR Reporting

- In order to produce reports related to Human Resources, a user must have the role of Agency HR - Report Generator. This role will only allow reporting from the authorized roles they have been assigned in HR (example: you must have the role of Agency Position Specialist in order to run position related reports).

Benefits

- Agency Benefits – Specialist (Benefits Billing) role would be assigned to an individual within an agency who is responsible for receiving payments from employees to pay for their health and/or life insurance coverage while they are on unpaid leave. They will have update access within the system to record payments as they are made by employees.

- Agency Benefits – Benefits Billing Viewer role is assigned to an individual within an agency who may need to review received payments from employees for their health and/or life insurance coverage. They will not have update access to the system with this role.

- Agency Benefits – Specialist role should be assigned to an individual within an agency responsible for setting up an employee’s health and or life insurance coverage, making changes to dependents/beneficiaries, processing Open Enrollment elections. This role does have update access to the system.

- Agency Benefits – Viewer role would be assigned to an individual who has a need to know what an employees health or life insurance elections are but is not responsible for maintaining this information in the system. This role does not have update access to the system.

Payroll

- Agency Payroll – Report Generator role would be used by agency payroll staff to obtain reports from the system. It may also be useful to the fiscal office within an agency to allow their financials staff access to payroll records.

- Agency Payroll – Specialist role is used by the individuals within an agency responsible for maintaining their employee’s payroll data, including Additional Pay payments, Direct Deposit, Deductions and Tax setup. It does have full update access to the system for payroll data. It also grants access to view an employee’s garnishment data where applicable as well as paycheck data, earnings and tax information but does not have update access to the system for this purpose.

- Agency Payroll – Viewer role is used by individuals within an agency to view their employee’s payroll information. It does not have access to an employee’s garnishment information where applicable. It also does not have update access to the system. This role is useful to those individuals who are responsible for financial reporting within their agency.

Time & Labor Security

PeopleSoft HRMS Time & Labor module allows the definition of row security Permission Lists that give the users affiliated with selected Permission Lists the authority to:

- Enter or update time reported in a previous period.
- View and enter data for time reporters who belong to the dynamic groups that are specified. This feature is called Group Security.

Dynamic Groups are comprised of time reporters who met the group selection criteria as of the time the dynamic group was last refreshed. When an employee leaves or enters this selection criteria they are added or removed from the dynamic group the next time that the dynamic group is refreshed. Typically, this process is executed on a nightly basis.

With Dynamic Group Security enabled, timekeepers (those who enter time into the system) can only view time reporters (employees) who are members of the Dynamic Group that are assigned to their row security Permission List. A timekeeper defaulting to department security can only enter time for time reporters in the same department they are in.

Notes about Specific TL Roles

- Agency TL Specialist is responsible for administering Time and Labor functions. This role has access to all aspects of the Time and Labor module including agency-wide batch reports. This role is typically given to the Payroll supervisor.
- Agency Timekeeper Specialist is responsible for time entry and adjustments. This role includes access to employee set up pages for schedules, leave plans, and compensatory plans.
- Agency Timekeeper role has limited access to Time and Labor. The main function of this role is time entry and adjustment. A modified Agency Timekeeper role exists that does not allow processing of prior period adjustments.
- Agency TL Leave Plan Specialist manages leave plan activity. This role is responsible for enrolling employees in leave plans, reviewing leave balances and reviewing leave plan criteria.
- Agency Time Reporter relates to self service time entry only. This role enters and views his/her/his own time.
- Agency Approver relates to self service time entry only and has the primary function of approving time entered by other employees. Access is also granted to enter time, view time, manage schedules, and manage exceptions for the dynamic groups assigned.
- Agency TL Report Generator can produce reports for the dynamic groups they have access to.
- Agency TL Viewer can view all aspects of the Time and Labor module including HR Job Data. This role is typically given to HR employees.

EPM Security

Overview

The EPM tool contains a number of Financial and HRMS Reporting Tables that were developed by the EPM team. These Reporting Tables are denormalized versions of delivered PeopleSoft tables. The idea was to make it easier for users to develop reports by consolidating that data into fewer tables.

Data and Pages are secured through a variety of ways. All EPM users will receive the following two roles in EPM which drive their page and non-page access:

CT EPM USER - Grants access to all Non-Page Permissions (Web Libraries, Component Interfaces etc.), the EPM Data Dictionary and the PS Query tool.

CT EPM PRIVATE - Allow a user to create only Private Queries. This means no other user will have access to see, modify, run or delete this users report.

The user will be given access to data based on the Financials Roles they have and based on their Primary Permission List. If a user has the ability to navigate to any page within a given module that user will be granted the ability to query off every Reporting table in that module. For instance, if a user has the Vendor Viewer Role, they have access to all Accounts Payable Reporting Tables. This access is allowed through the EPM Query Tree by assigning certain Accounts Payable reporting tables to an Accounts Payable Tree node which is associated with Permission Lists and corresponding roles.

Just as in Financials and HRMS, a user is granted a Primary Permission List which identifies what Financial Business Units or HR Departments they can view. This permission list restricts the results of the queries to these Business Units or Departments assigned.

Useful Links

The HRMS CO-1092 – Application Security Request Form – Completion Guide for Liaisons and Approving Managers
http://www.core-ct.state.ct.us/security/hrms_sec.html

The Financial CO-1092 – Application Security Request Form – Completion Guide for Liaisons and Approving Managers
http://www.core-ct.state.ct.us/security/fin_sec.html

On-line CO-1092 Addendum Form and Procedures
http://www.core-ct.state.ct.us/security/proc_updates.html

Workflow Routings Job Aid - Security Liaisons
http://www.core-ct.state.ct.us/financials/wf/job_aid-security_liaisons.doc

Workflow Routings Job Aid - Users
http://www.core-ct.state.ct.us/financials/wf/job_aid-core-ct_user.doc

HRMS Role Handbook
http://www.core-ct.state.ct.us/security/pdf/hrms_role_handbook_task_55_9_1.pdf

Financial Role Handbook
http://www.core-ct.state.ct.us/security/docs/financials_role_handbook.doc

Financial Role Matrix
http://www.core-ct.state.ct.us/financials/ap/xls/sgrgtn_dutis.xls

Financials Agency Security Liaisons List
http://www.core-ct.state.ct.us/security/xls/scrty_liaisons.xls (Financials tab)

HRMS Agency Security Liaisons List
http://www.core-ct.state.ct.us/security/xls/scrty_liaisons.xls (HRMS tab)

Liaison Password Reset Instructions and FAQs
http://www.core-ct.state.ct.us/security/proc_updates.html

Password Security Policy
http://www.core-ct.state.ct.us/support/password.htm

EPM Queries for Security Liaison Reporting
https://www.core-ct.state.ct.us/reports/CP-REPORTS-epm_select.aspx?minorCat=Security