CO-1092 Completion Guidelines (Electronic)

1. The supervisor of the unit initiates and authorizes the request, and forwards it to the agency liaison.

2. The CO-1092 Liaison reviews the request, and navigates to the CO-1092 Entry page.

    a. HRMS Navigation: Main Menu > Core-CT HRMS > PeopleTools > Security > CO-1092 Security Request

    b. Financial Navigation: Main Menu > Core-CT Financials > PeopleTools > Security > CO-1092 Security Request

3. On the CO-1092 Security Request page, the liaison will select the Add a New Value tab and type or select the User ID, and click Add. The CO-1092 Security Request page will display.

4. The User ID information is already displayed. The liaison will select an Approving Manager from the Manager User ID look up.

    a. HRMS: Row Security, Edit Departments, and Edit TL Groups should be supplied by the liaison. If the Row Security is not known, it may be left blank.

    b. Financials: Primary Permission and Edit Business Units should be supplied by the liaison. If the Primary Permission is not known, it may be left blank.

5. The liaison will type or select roles in the Security Roles (Add/Delete) section. This section is includes the Role Name, Role Action (Add/Delete dropdown), and description (supplied once the role is selected).

    a. There is a Comments tab should additional information be required.

    b. The Comments tab can also be used to attach additional documentation.

6. Once roles have been selected and optional comments made, the liaison will click the Submit button to send the request to the agency's CO-1092 Approving Manager.

7. The CO-1092 Approving Manager may only Approve or Deny the request. Once approved, the request is submitted for central review.

    a. Additionally, the approving manager may review or add comments on the Comments tab.

Points to remember when filling out the automated CO-1092 Security Request Form:

1. The automated CO-1092 replaces both paper forms carrying the same name.

2. If a user has both HRMS and Financial roles, two requests need to be submitted.

3. The EPM private and public (superuser) roles are selectable for both automated forms.

4. Once an automated CO-1092 is submitted, it receives a transaction numbers. Transaction numbers are assigned on a statewide basis.

5. There is a Viewing Existing Roles link so the liaison can view the roles a user has without having to leave the CO-1092.

6. An automated CO-1092 can be saved for later completion.

7. Role Names can have one of three descriptions

    a. This is a Valid Role

    b. Segregation of Duties Conflict

    c. The User Profile already has this Security Role.

8. OSC has stated that they will deny any Financial CO-1092 that contains conflicting roles. Agency Security Liaisons should research the user's profile and ensure forms with conflicts have the necessary Delete/Add combinations and Agency Liaisons should remove the conflict upon receiving the warning message.

9. OSC requires agencies to submit a new or updated CO-512 when requesting any final approval roles within five days. If this process is not followed, the CO-1092 will be denied. This form can be found at: http://www.osc.ct.gov/agencies/forms/excel/CO-512Rev04-2006.xls

10. OSC is requiring that the Financial Appendix Page be used and attached when updating Origins, AP/PO Business Units, Ship-to-Locations, etc. The comments page should NOT be used for identifying this information. This form can be found at: http://www.core-ct.state.ct.us/security/xls/fin_appdx.xls.

11. Financial roles requiring either a CO-512 or a Financial Appendix are

    a. General or Program Buyer

    b. Purchase Order Amount Approver 1, 2

    c. Purchase Order Budget Approver (CO-512 also required)

    d. Requester

    e. Catalog Viewer

    f. Requisition Amount Approver 1, 2, 3, 4

g. Requisition Budget Approver

h. Requisition Purchasing Approver (CO-512 also required)

i. Alternate Approver (CO-512 also required)

j. Adjustment Voucher Processor

k. Journal Voucher Processor

l. Voucher Maintenance Processor

m. Voucher Processor

n. Voucher Approver (CO-512 also required)

12. For more information on Roles requiring route controls values, please go to the Core-CT Security Website: http://www.core-ct.state.ct.us/security/

13. Once submitted, the automated CO-1092 creates an Approval Routing. This routing can be used by liaisons to track the progress of a request. Approvals and denials are date stamped.

14. At each step, an email is generated to the next level indicating that a request is awaiting action.

    a. Core-CT Security is always the last step in the CO-1092 workflow. When the request is submitted by Core-CT Security, an email is generated to the originating liaison indicating that the profile is active for the user.

    b. Roles can be removed at any level except Approving Manager. If a role is removed during the central review process (in consultation with the liaison), an email is generated to the liaison indicating the role has been removed.

15. Comments may be added at any approval step. The most recent comment is always first.

    a. When a comment is added, the previous comment is duplicated. This duplication may be deleted.

16. The liaison can view every user in the state when they select a user for the automated CO-1092. However, they can only select users to whom they have access.

Security inquiries and password resets must be emailed to corect.security@ct.gov