SEAN SCANLON
STATE COMPTROLLER

TARA DOWNES
DEPUTY COMPTROLLER

STATE OF CONNECTICUT
OFFICE *of the* STATE COMPTROLLER
165 Capitol Ave.
Hartford, CT 06106

MEMORANDUM NO. 2025-11

JUNE 4, 2025

TO THE HEADS OF ALL STATE AGENCIES

Attention: Chief Administrative and Fiscal Officers, Business Managers, and Payroll and Human Resources Officers

Subject: Comptroller's Core-CT Systems Security for State Employees

I. PURPOSE

This memo replaces memoranda 2014-19. The purpose of this memo is to advise all state agencies of the importance of having appropriate internal controls over and within the Core-CT Financial and Human Resource Management System (HRMS) to ensure that all transactions are properly authenticated and authorized. Guarding against unauthorized and inappropriate access to the Core-CT system is critical because of the integration of the Financial and HRMS Systems. Unrestricted access to the Core-CT system compromises the controls provided by segregation of duties and other safeguards that are part of manually operated systems.

II. CONTROL ACTIVITIES

Security in the Core-CT system is imperative and must be restricted to only those individuals authorized to have access. The initial request for user access to Core-CT is done via the Financial and HRMS Forms CO-1092, Agency Application Security Request Form, which has been automated in Core-CT.

Each agency has the responsibility to assign a Core-CT Agency Security Liaison to be the primary contact with the Statewide Core-CT Applications Security Administrator. The Agency Security Liaison is responsible for monitoring all authorized access to the Core-CT Financials/HRMS application and acting as point of contact for the Core-CT Applications Security Administrator. One or more backup Agency Security Liaisons should be assigned to ensure an immediate response to secure the integrity of the Core-CT Financial System if an agency becomes aware of a need to remove access. Each agency is responsible for developing internal security procedures for Financial, HRMS, and EPM users.

III. RESPONSIBILITIES

A. Central Oversight Agencies (OSC Core-CT, OSC CAP, DAS HR):

- An on-going audit of agency HRMS and Financial roles is conducted by the State Comptroller's Accounts Payable Division, Budget & Financial Analysis Division, Payroll Services Division and Core-CT staff of both the State Comptroller and Department of Administrative Services for compliance with segregation of duties and standards of access. Failure of the Agency Security Liaison to properly administer their duties could result in the removal of roles or deactivation of UserIDs in Core-CT.

B. Agency Security Liaisons:

- Work with their agency's unit supervisors or managers to ensure the proper roles are assigned and user access is appropriate. Depending on the agency's organizational structure, employees may have one or more roles. In addition, more than one employee may perform the same role within an agency.
- Assure, along with unit supervisors or managers, that there is proper segregation of duties for the roles assigned.
- Submit all requests to change, add, or delete roles and/or access using the on-line CO-1092, Agency Application Security Request Form.
- Remove access immediately upon the notice of an employee's termination, retirement, or transfer to another department/agency. When an employee transfers from one agency to another, the employee's ID is reusable, but Core-CT access must be reinstated by the new agency.
- Maintain system integrity by training users in the confidentiality of user IDs and passwords, monitoring for credential use violations, and immediately removing access from anyone who violates credential guidelines.
- Reset user passwords when necessary and ensure system profiles are set up with valid email accounts. Update user email addresses if incorrect or missing.
- Train and enforce users setting up their system profile to utilize the automated password reset feature.
- Audit, at least quarterly, agency users' access and roles. Notify the supervisor or manager of any issues. Issues which violate segregation of duties, or the integrity of the system, shall be immediately resolved by the security liaison.
- Contact Core-CT Application Security Administrator with any questions regarding user IDs, passwords, roles, or access.
- Review all related on-line security documentation on the Core-CT website at https://www.core-ct.state.ct.us/security. If there are any questions

regarding the information provided on Core-CT, please contact CoreCT.security@ct.gov.

Liaisons may share these responsibilities and tasks only with other authorized liaisons within their agency. Core-CT Security Administration will not communicate security information to unauthorized agency personnel.

C. Agency Supervisors and Managers Shall:

- Review the access of all users under their authority and restrict that access whenever it is incompatible with the user's work role and/or does not provide proper segregation of duties.
- Approve only the roles and user access required by their staff to perform the business functions of the agency.
- Enforce that user IDs and passwords are not shared for convenience between personnel.
- Instruct staff to change passwords immediately if they suspect that the security of such passwords has been compromised.
- Correct user access when an employee has a change in responsibility within the agency.
- Promptly respond to quarterly, or intermittent, audit requests by the agency security liaison regarding staff duties.
- Verify that the security liaison has submitted the CO-1092 to lock out user account access immediately upon the notice of an employee's termination, retirement, or transfer to another department/agency and take any actions to process that request.

Agency Human Resource staff must provide advance or immediate notification to the agency security liaison of an employee's termination, retirement or transfer to another department/agency. Agency Security Liaisons should remove access on the date of separation, or immediately, as directed by Human Resources.

D. All Agency Employees are Responsible to:

- Ensure that their user IDs and passwords are not shared with anyone for any reason.
- Ensure that their user IDs and passwords are not attached to terminals, desktops, or located where unauthorized personnel may obtain access to them.
- Ensure that passwords are changed immediately if the employee suspects that the security of his/her password has been breached.
- Set up their system profile to utilize the automated password reset feature.
- Report to their supervisor, manager, and agency security liaison if they become aware of roles or access under their user ID that does not align with their job duties.

IV. PROCEDURES

The following are the procedures for submitting the on-line CO-1092 security application requests.

1. The supervisor or manager of the unit initiates the request, and forwards it to the agency security liaison. Agencies will develop a procedure for requesting roles and user access as part of their agency security procedures.

2. The liaison reviews the request and verifies that the requested roles and user access assigned are appropriate. Then the liaison enters the request into Core-CT's electronic CO-1092. The liaison clicks on the submit button to route the CO-1092 triggering a workflow process that sends the request to the designated approving manager for review and approval.

3. Once the CO-1092 has been submitted, the approving manager will receive a request to approve the CO-1092 in Core-CT. The approving manager reviews the CO-1092 for accuracy and, if it is correct, approves it. The CO-1092 is then automatically sent for the appropriate Central Authorization before the request is processed. If proper segregation of duties is maintained, the request is approved. If not, it is denied. Under no circumstances will the submitted CO-1092 be altered by any of the Central Authorization staff or the Core-CT Security Team. If there is information missing on the appendix page, agencies will be allowed to submit a new appendix page.

   NOTE: Policy for Financial Roles — If an agency submits a security request for a new employee or changes to an existing employee's role for "Final Approver" in encumbrance or expenditure, they must submit an updated Claims Authorization Form (CO-512) to the Office of the State Comptroller, Central Accounts Payable Division, osc.apd@ct.gov, before the security request can be approved.

4. Core-CT Security Administration will process the request and communicate the completion to the agency security liaison and communicate with the security liaison a temporary user ID and password, if applicable.

5. The retention period for any original records related to CO-1092's is two years from the date that an employee separates from the agency. The original copy is retained by the submitting agency. Destruction can occur after the minimum retention period and submission to the State Library for approval of form RC-1000.

V. PASSWORD SECURITY POLICIES

Authorized agency security liaisons are responsible for resetting passwords for users in their agencies if a user is locked out or the liaison becomes aware of a compromised login. The automated password reset feature is on the Core-CT logon page. 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 numeric.
- The previous six (6) passwords are retained in the system and cannot be reused.
- Alphabetic, numerical, and certain special characters are allowed.
- Passwords should be obscure rather than obvious.
- Longer passwords are generally more secure.
- 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.

User IDs and passwords should be hand delivered or emailed by the agency security liaison. Agency personnel should be informed-of the password guidelines, agency policies, procedures regarding password and access problems, and who to contact for assistance.

Any problems associated with user IDs or passwords must be communicated through the agency security liaison. Agency personnel are not to contact the Core-CT Security Administration directly.

VI. QUESTIONS

Questions regarding On-Line CO-1092 processing and general assistance may be directed to your Agency's Security Liaison. A list of Liaisons can be found at http://www.core-ctstate.ct.us/security.

Questions regarding Memorandum Interpretation and Security Procedures and Internal Controls, or central review of requests (Segregation of Duties) can be directed to the State Comptroller's Office, Central Accounts Payable Division, Security & Asset Management Unit at osc.security@ct.gov.

DocuSigned by:

03479587B0B543C...

SEAN SCANLON
STATE COMPTROLLER

SS:PM
https://www.osc.ct.gov