DocuSign Envelope ID: BDA39A93-89CF-4A06-8810-BD6883DF5C1E

SEAN SCANLON
STATE COMPTROLLER

TARA DOWNES
DEPUTY COMPTROLLER

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

MEMORANDUM NO. 2023-22

November 3, 2023

TO THE HEADS OF ALL STATE AGENCIES

Attention: **Business Managers, Human Resource Officers, and HRMS/FIN Security Liaisons**

Subject: **Non-Standard Core-CT Access and User ID Creation**

I. PURPOSE

The State Comptroller’s Office is charged with maintaining the security and integrity of the CORE-CT financial system. This memorandum sets policy for requesting non-standard access to CORE-CT, informs agencies of changes to procedures for requesting non-standard access or user IDs, and lists required forms needed to make those requests.

II. AUTHORITY

CT General Statutes Sec. 3-112– **Powers and Duties.** The Comptroller shall: [….] (4) prescribe the mode of keeping and rendering all public accounts of departments or agencies of the state and of institutions supported by the state or receiving state aid by appropriation from the General Assembly; (5) prepare and issue effective accounting and payroll manuals for use by the various agencies of the state;

CT General Statutes Sec. 3-115a – **Providing for budgetary and financial reporting needs of the executive branch.** The Comptroller, in carrying out accounting processes and financial reporting that meet constitutional needs, shall provide for the budgetary and financial reporting needs of the executive branch as may be necessary through the CORE-CT system.

III. RELATED POLICIES

This memorandum supplements the previously published policies,
Comptroller’s Core-CT Systems Security for State Employees - Memorandum No. 2014-19 and
Core-CT Access for Non-State Employees – Memorandum No. 2022-07,
with additional procedures related to required forms. Those previously published policies are still in effect and updated procedures are included in this memorandum.

IV. POLICY

Each agency must establish internal policies and procedures to maintain adequate internal controls following the guidance provided by the State Comptroller’s Internal Control Guide (ICG) and ensure all financial transactions are properly authenticated and authorized. Guarding against unauthorized and inappropriate access to the Core-CT system is critical to maintaining the integrity of the state’s financial system and preventing fraud and misuse of taxpayer funds. Agencies are responsible for assigning a Core-CT Security Liaison to be the primary contact with the Statewide Core-CT Applications Security Administrator. The security liaison is responsible for monitoring all authorized access to the Core-CT modules and acting as the primary agency contact for Core-CT applications.

a. **Issuance of Multiple User IDs for Core-CT**
Due to the way security roles are set up in Core-CT, it is sometimes necessary to provide users with separate profiles so that their roles do not allow them to transact in violation of internal controls. When a security liaison detects a potential conflict in a user's security request, a secondary profile may need to be established. Security liaisons who believe a conflict could exist should contact osc.security@ct.gov for guidance before submitting a request for multiple User IDs.

Ex. IR User IDs where an agency user needs to be able to maintain refund vendor profiles, but they cannot be granted that on their normal profile because it would allow them to modify central accounts payable vendor profiles.

b. **Portal Access Outside Normal Hours**
Core-CT system security is imperative, and access must be restricted to only state employees and other individuals authorized for specific business needs. The Comptroller's Core-CT Division has the ultimate authority for granting access to the Core-CT Financials and HRMS systems as they are responsible for the overall integrity of both.

Agencies must document and submit a clear justification for after-hours access and obtain approval from OSC Security. Batch and maintenance processes run after hours and users who are granted access will not be allowed to perform certain transactions during these processes to maintain the integrity of the state financial system.

c. **Core-CT System Security**
All users must be informed of, and comply with, relevant State electronic use policies which may include, but are not limited to the following:

- Acceptable Use of State Systems Policy (ct.gov)
- Policy on Security for Mobile Computing and Storage Devices (ct.gov)
- Network Security Policy and Procedures (ct.gov)
- Health Insurance Portability and Accountability Act

V. PROCEDURES

a. **State Employee Multiple User ID Request:**
To request an additional "secondary" User ID the agency security liaison must fill out the State Employee Multi-User ID Core-CT Access Request Form CO-1091-MU Core-CT FIN Security (state.ct.us) and email the completed form to osc.security@ct.gov. The agency must include the justification/purpose for the secondary User ID in the justification box provided on the form. OSC Security will review the form and justification. OSC Security will send to Core-CT Security who will create a separate, secondary logon, User ID and password. Once the User ID is established, Core-CT will note the new USER ID on the CO-1091-MU and email the completed form to the agency with a copy to osc.security@ct.gov. The agency security liaison will then use the new secondary User ID when creating an online CO-1092 request for roles, place a note on the comments page "Approval on file with OSC Security" with the date they received the approved email, and attach a FIN Appendix page if applicable. When requesting roles, a segregation of duties compliance evaluation should be performed on ALL user ID's.

b. **Non-Standard Hours Access Request: (This approval is very limited.)**
To request after-hours access, the Agency Head or designee should complete the 24-Hour Creation/Access form CO-1091-24 Core-CT FIN Security (state.ct.us) and email it to osc.security@ct.gov. The agency must include the justification/purpose for the Non-Standard Hours in the justification box provided on the form. OSC Security will review the form and justification. If approved, OSC Security will forward the form to Core-CT who will review the roles associated with the request. If Core-CT denies the request, they will notify the agency via email with a copy to osc.security@ct.gov and attach the denied form. If Core-CT Security approves the request, they will create a separate (Secondary) logon user ID with a 247 prefix and password. Once the secondary ID has been created, Core-CT will email the agency and osc.security@ct.gov of the approval and attach the approved signed form with the secondary ID listed on the CO-1091-24 form. The agency security liaison will then select the secondary ID when creating an online CO-1092 request for roles, place a note on the comments page "Approval on file with OSC Security" with the date they received the approved email, and attach a FIN Appendix page if applicable.

VI. REFERENCES

All forms are available to be downloaded from the Comptroller's Forms page under the State Agency Resources tab on the Comptroller's website at http://www.osc.ct.gov

VII. QUESTIONS

The questions section should give pertinent contact information for clarification. It should also include email contacts or links to online help. Ex. Questions regarding this Memorandum or the completion of the forms should be directed to osc.security@ct.gov.

DocuSigned by:
03479587B0B543C...

SEAN SCANLON
STATE COMPTROLLER

SS:HR
http://www.osc.ct.gov