

SEAN SCANLON
STATE COMPTROLLER



TARA DOWNES
DEPUTY COMPTROLLER



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

MEMORANDUM NO. 2024-03

January 23, 2024

TO THE HEADS OF ALL STATE AGENCIES

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

Subject: Non-State Employee Core-CT Access

I. PURPOSE

The State Comptroller's Office is charged with maintaining the security and integrity of the Core-CT financial system. This memorandum establishes the policy for requesting non-state employee access to Core-CT and the required form needed to make the request.

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 supersedes the previously published policy, [Core-CT Access for Non-State Employees](#) – Memorandum No. 2022-07, with new procedures related to this process.

IV. POLICY

Access to the Core-CT system is restricted to state employees and other individuals authorized for a specific business need. Some examples of non-state employees are consultants, interns, temporary workers, or agents acting on behalf of the state.

Financial approval roles in Core-CT will not be granted to non-state employees. Sharing of user IDs and passwords is prohibited. Access to the state's internet is to be limited to the information that is needed to perform the job function and supported by a written contract or agreement.

State equipment is to be used where possible. All data remains the property of the State of Connecticut and is not to be downloaded or housed on non-state equipment. State equipment,

data, and other items must be protected at all times. Users must take measures to prevent unauthorized disclosure or damage. This requirement is to be applied at the official duty station, any other work location, and when transporting between locations.

Agencies requesting non-state employee access to Core-CT must establish a policy based on this memo, comply with OSC memorandum 2014-19, and maintain adequate internal controls. A clear justification must be documented. Detailed records (name, address, work history, etc.) must be maintained. Agencies must verify the individual's identity with a government issued ID.

Core-CT System Security

All users must be informed of, and comply with, relevant State electronic use policies which 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

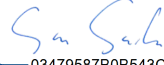
a. Non-State Employee User ID Request:

- i. To request Non-State Employee Access, complete the Non-State Employee Creation/Access form CO-1091-NSE [Core-CT FIN Security \(state.ct.us\)](#). The agency must include the justification/purpose for the non-state employee in the justification box provided on the form. Email completed forms to osc.security@ct.gov.
- ii. OSC Security will review the form and justification. If approved, OSC Security will submit to Core-CT for review. Rejections will be returned to the agency by email.
- iii. If Core-CT approves, they will set up the NSE User ID with just the necessary dynamic roles. Rejections will be returned to the agency by email.
- iv. Once the NSE User ID is established, Core-CT will note it on the CO-1091-NSE form and email to the agency and cc: OSC.security@ct.gov.
- v. The agency security liaison should then submit an on-line CO-1092 using their User ID and will check the NSEU box on the CO-1092 when requesting the necessary roles. Once the NSEU box is checked, the User ID field will become available. The security liaison will enter the NSE User ID provided on the CO-1091-NSE form.
- vi. The security liaison will attach the CO-1091-NSE form to the comments tab of the CO-1092, select the roles (proper approval workflow is triggered), add the same required roles in the comments section and submit.
- vii. Core-CT Security will confirm the CO-1091-NSE form is attached to the CO-1092 and all approval levels are properly completed. Core-CT Security will add the requested roles to the newly created profile listed on the CO-1091 and will delete the selected roles from the liaison's CO-1092 prior to approving the CO-1092. The roles will remain in the comments section for audit purposes.

The security liaison is responsible for non-state employee security management. When a non-state employee's roles or assignments change, the access must be adjusted. Access to Core-CT must be removed immediately when the non-state employee is terminated. Periodic audits of agency non-state employee roles should be performed to insure appropriate access.

VI. 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:MH

<http://www.osc.ct.gov>