

Central Payroll System Security Policy

Overview

The Central Payroll System security procedure establishes levels of controls for each user based on that user's job function, per agency request. These levels of controls prevent system access by unauthorized operators, prohibit access to restricted data and protect the physical products of the system.

The OSC Central Payroll Division Security Administration Team is responsible for:

- The definition of forms and procedures for identifying and tracking authorized operators.
- The maintenance of statewide security profiles for operator access based on job requirements and functions.

Expectations/Deadlines

Security Administrators

All agencies must submit the Central Payroll System Security Letter before the OSC Central Payroll System Security Administrator approves the agency's use of the Central Payroll System. The agency's Chief Executive Office and Chief Financial Officer must sign the security letter and the letter should be submitted on the agency's letterhead.

The Authorized Agency Security Administrators Letter from the OSC must be completed and signed by the authorized agency security administrators and returned to the Central Payroll Division.

Note: Both the Central Payroll System Security Letter and the Authorized Agency Security Administrators Letter should be completed as agency security administrators change during the year. These forms are maintained in the system security log for reference as additional requests are received. Letters received will not be accepted if any signatures on the letters are not original (no signature stamps are acceptable). Security request forms received will not be processed if the signature provided is not original (no signature stamps are acceptable) and is not one of the authorized security administrators listed on the file form. These forms will be updated annually, even if no changes occur.

Security Forms/Requests

Security request forms are available online at the Central Payroll Division web site under the Security topic:

http://www.ncosc.net/sigdocs/sig_docs/payroll/index.html

Security requests may be submitted via email if the sender is a valid agency Security Administrator and the requestor provides their RACF ID number, or the requests can be faxed to (919) 981-5570. Faxed forms must contain signatures (not signature stamps) of

a valid agency Security Administrator. Forms will be processed on the same day received.

All agencies must have at least two Security Administrators. Security Administrators are not permitted to sign their own security forms requesting changes to their security. The agency CFO or CEO responsible for signing the Central Payroll Security letter must sign for a security administrator's changes.

Periodic Review

Agencies and universities are required to review current security data and certify semi-annually that the information provided in the agency or university's security report is accurate and submit any required changes, as appropriate. Security reports are generated quarterly and are available through Systemware under the report name:

OSCPX CENTRAL PAYROLL ACCESS REP

Responsibility for the Protection of Personal Data

All individuals responsible for requesting security access to the Central Payroll System are required to be aware of and confer on all security applicants the sensitive nature of the data available through the Central Payroll System. It is the responsibility of agency CFO/CEO's and security administrators to notify all users of the Central Payroll System that personal identifying information such as social security numbers are obtained as part of the data gathering process for this system. By requesting access to this system, all agents responsible for Central Payroll System access must agree that any information made available will be used for business purposes only, as it relates to the specific job functions of the personnel accessing the system. It is an attestation that the system and system-related information will not be shared, disseminated, or used in any way other than their original intent.