STATE OF CONNECTICUT
Department of Mental Health & Addiction Services

dmhas
A Healthcare
Service Agency

Commissioner's Policy Statement and Implementing Procedures

SUBJECT:	CORE-CT Financial Security Liaison Role
P & P NUMBER:	Chapter 5.2
APPROVED:	Miriam Delphin-Rittmon, Commissioner Date: 10/15/2015
EFFECTIVE DATE:	October 15, 2015 Miriam Delphin-Rittmon
REVISED:	9/1/2012, 8/15/2012
REFERENCES:	
FORMS AND ATTACHMENTS:	

STATEMENT OF PURPOSE: To Establish internal security procedures for CORE-CT Financials application.

POLICY: DMHAS recognizes the importance of having appropriate internal controls over the Core-CT Financial System to ensure that all transactions are properly authenticated and authorized. Guarding against unauthorized and inappropriate access to the Core-CT system is critical. 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.

The DMHAS Security Liaison is responsible for monitoring all authorized access to the Core-CT Financials application to their agency personnel and acting as point of contact for the Core-CT Applications Security Administrator.

PROCEDURE:

Responsibilities of the DMHAS Financial Security Liaison

- Requesting new access for system users and changes to existing access.
  - Review each user's access and restrict that access where the access is incompatible with the user's job description and/or does not provide proper segregation of duties. Approve only the employees required to perform the business functions.
  - Correct user access when an employee has a change in responsibility within the agency.

- Submit all new, change, or delete requests on the CO-1092, Agency Application Security Request Forms.

➢ Requesting deletion of 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 has to be re-defined by the new agency.

➢ Maintaining confidentiality of User-ID's and passwords.

- Enforce that User-ID's and passwords are not shared for convenience between personnel.
- Enforce that User System Profiles are set up to leverage the automated password reset process and include valid email accounts.
- Enforce that User-ID's and passwords are not attached to terminals, desktops, or located where accessible to unauthorized personnel.
- Enforce that passwords are changed immediately if the employee suspects that the security of his/her password has been breached.

➢ Resetting User passwords when necessary and ensuring system profiles are set up and include valid email accounts.

➢ Contacting Core-CT Application Security Administrator with any questions regarding User-ID's, passwords or access.

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

Guidelines and procedures for submitting security application requests.

(The Core-CT Application Security Request Forms (CO-1092) are available at: http://www.core-ct.state.ct.us/security/xls/finform.xls).

➢ The supervisor of the DMHAS unit initiates and authorizes the request via an email to the Financial Security Liaison. The DMHAS Financial Liaison completes and signs off on the CO-1092.

➢ The liaison **must fax** the request to the Core-CT Security Administrator at **(860) 622-2611 and retain the original at the agency for auditing purposes.**

➢ Core-CT will obtain the appropriate Central Authorization before the request is processed. In addition, an on-going review of agency financial roles is conducted by the State Comptroller's Fiscal Policy Division, 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.

➢ Core-CT Security Administration will process the request and communicate the completion to the DMHAS Financial Security Liaison with the User-ID and password, if applicable.

- Retention period for the CO-1092's is two years from the date that an employee separates from DMHAS. Original copy is retained by DMHAS. Destruction can occur after minimum retention period and submission to the State Library for approval of form RC-108.
- If DMHAS submits a security request for a new employee, or changes to an existing employee's role for "Approver" in encumbrance or expenditure, DMHAS must also submit an updated Claims Authorization Form (CO-512) to the Office of the State Comptroller, Accounts Payable Division before the security request can be approved.

Password Security Policies and Procedures

- All passwords expire in sixty (60) 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 can not match the User ID.
- The password must be at least eight (8) characters in length, three (3) of which must be digits. Six (6) passwords are retained in the system and passwords cannot be reused.
- Both alphabetic and numerical characters are allowed.
- Passwords should be obscure rather than obvious.
- 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. The following is the link for instructions on setting up the user profile: http://www.core-ct.state.ct.us/security/pps/pwreset.pps

Resetting Passwords

- Only authorized Agency Security Liaisons have the ability to reset passwords in DMHAS.
- When a user requests a password reset, the Liaison will:
  - Check in CORE to see if the User has set up their user profile and if so, check to make sure the email address is correct.
  - If the user profile has been set up, the user will be instructed to use the Forgot My Password Link.
  - If not, the Liaison will reset the password and instruct the user on how to set up their profile in the system.