

Rules for using the Protective Enclave

Scope: SO, CCC	Revision Date: 12/4/2017
Approved by: Joe Tolisano, CIO	Approved on date: 12/4/2017

Table of Contents

1. Introduction	1
2. Purpose	1
3. Usage Provisions	1
4. Compliance	2
5. Data Access Responsibilities	2
6. Related Publications.....	2

1. Introduction

The Protective Enclave is a physical and/or logical separation of applications, systems and networks that process DCL3 data. The Protective Enclave provides a high security computing environment for the limited number of Faculty/Staff that process DCL3 data at the colleges and the CSCU System Office. In the past, DCL3 data was accessed from applications running directly on workstations. Now, DCL3 data must only be accessed from inside the CSCU Protective Enclave using applications launched from a virtual desktop.

The Protective Enclave requires additional security controls and restrictions to ensure the application and data remain protected. When accessing the Protective Enclave, Faculty and Staff will login through a secure channel to access to a virtual desktop. Once logged onto the virtual desktop, you will be able to access/work with DCL3 data (e.g., Banner, secure websites, documents contain confidential information, etc.). DCL3 data will not be able to leave the Protective Enclave.

2. Purpose

This document describes the responsibility for using the Protective Enclave.

3. Usage Provisions

The following are the Protective Enclave usage provisions:

- The usage of the Protective Enclave is subject to all CSCU policies and standards, including the [Acceptable Use Policy](#), the [Information Security Policy](#) and the [Data Management Standard](#).
- Regardless of where documents reside, they are still considered state records and must be kept in compliance with State of Connecticut Record Retention Schedules (see [Data Management Standard](#) for more details).
- Accessing applications that provide dual functions (access to DCL3 data and access to non-DCL3 data) for example: CORE-CT, must only be used for accessing non-DCL3 data when outside the Protective Enclave. Using the application to access DCL3 data must ONLY be done from within the Protective Enclave.
- When printing documents from the Protective Enclave, use the following usage provisions:
 - Verify the location of the printer you are printing your documents to make sure it is the correct printer.
 - Do not let the documents sit at the printer; pickup your documents shortly after printing DCL3 data at the printer.
- When working with documents in the Protective Enclave, if documents are known to contain DCL3 data, manually flag the data as containing DCL3 data using procedures outlined in the [Protective Enclave documentation](#). This flags the data as containing DCL3 data even if the DLP product cannot or is not able to identify that DCL3 data exists.
- Do not use screen capturing technology from your workstation or mobile devices to take screenshots/photos of DCL3 data and store it outside the Protective Enclave (i.e. on your workstation, on a mobile device, in a cloud service).

4. Data Access Responsibilities

Responsibilities for all users with access to CSCU Data:

- Protect CSCU data from unauthorized disclosure, corruption, or loss.
- Use CSCU data for legitimate and authorized purposes.
- Access only CSCU data for which you have been given authorized access.
- Employees will need to attend Data Management course as part of a comprehensive Information Security awareness program.

5. Compliance

Violations could result in loss of access to the Protective Enclave and appropriate disciplinary measures in accordance with local, state, and federal laws, as well as CSCU Policies, general rules of

conduct for all employees, applicable collective bargaining agreements, and CSU student conduct codes.

6. Related Publications

Related Policies

- [Acceptable Use Policy](#)
- [Information Security Policy](#)

Related Standards & Procedures

- [Data Management Standard](#)

Web Sites

- [Support Services Website](#)
- [Protective Enclave](#)