State Controller's Office Personnel and Payroll Services Division Decentralized Security Guidelines

Revised October 2020

Background

The purpose of these guidelines is to define the State Controller's Office (SCO) security requirements for all users of the SCO systems. Contact your department/campus Security Monitor for any questions or more information.

The SCO maintains the mainframe that houses numerous databases and systems of records, which contain confidential and sensitive data. Although the mainframe provides valuable information, access to centrally stored machine-readable data increases the risk of unwarranted disclosure of this data.

SCO maintains several automated security control systems, which will continue to be modified as needed, or when technology that is more sophisticated becomes available. However, individuals using or having control over data, which is confidential, or data, which could become confidential when associated with other data, must understand SCO requirements for handling such information.

Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in civil or criminal actions against those involved in the unauthorized disclosure (please refer to California Penal Code Section 502 and the California Information Practices Act). To reduce this risk, it is necessary for SCO to establish and enforce these requirements for all system users. Please read this document and the attached PSD108, Statement of Understanding, carefully to ensure comprehension before signing the form.

Controlling Access to Confidential Data

Access is granted to an individual based on these four factors:

- Be a current state employee and an employee of the requesting department/campus, AND
- Demonstrate either a job-related need to the information, AND
- Accept legal responsibility for preserving the security of the information (read the Decentralized Security Guidelines and sign the, PSD108 AND
- Receive formal approval from the PPSD DSA.

Once access has been approved, the individual is assigned a "User ID". The Security Monitor will be contacted by the SCO Information Security Office (ISO) to arrange processing of a password that will be known only to the individual. This unique password is the essential security system element that protects both the individual and data from unauthorized disclosure.

PASSWORDS: the individual owner must protect his/her password at all times. It is never to be disclosed to or "shared" with anyone. The failure to protect a password may result in a suspension from access to the SCO Personnel and Payroll systems. Any future failure to protect the password may result in permanent removal of access. (It should be noted that these actions are not to be misconstrued as punitive, but rather a corrective action and a safety precaution to limit further possible harm to the security of confidential data). Disciplinary or punitive action is determined on a case-by-case basis and may be in addition to other legal actions resulting from violating state law.

CAUTION: An individual may be considered to have "shared" their password if another individual uses an "active" terminal/PC under the following conditions:

- An individual, having logged on, leaves the active terminal/PC for an undetermined timeframe (i.e., break, lunch, and meeting) and another individual enters data or a transaction on the active terminal/PC.
- Either for "training" purposes or for someone who is waiting for access approval; an individual "logs on" to allow the other person to key enter data/transactions.

Once an individual logs on the system, all transactions or data keyed in under that individual's User ID/password are the responsibility of that individual, regardless of the circumstances or the legality of the information entered. The liability for any illegal transactions belongs to the owner of the password and the person who entered the transaction. Therefore, each individual must log off (deactivate a session) prior to leaving a terminal/PC.

Such liability may result in civil and/or criminal actions and be punishable under Section 502 of the California Penal Code.

PC 502 (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

The punishment for violating 502(c) (1) is stated in 502(d) (1), stated as follows: (d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

Responsibility for Protecting Confidential Data

The responsibility for protecting confidential and sensitive data residing on the SCO system is a shared effort. The SCO has a limited role in the total security effort. The SCO's responsibility encompasses the area of data, applications and access security. The area of access security at the initial point resides with department management selecting and requesting access for an individual who meets the criteria, previously mentioned. This responsibility, including protection of access (passwords), is straightforward and easily understood.

The responsibility that is less easily understood is the level of protection of confidential data that is either viewable on individual video monitors or extracted from a printer from the SCO system. This data, once it is removed or viewable within the department's Personnel and Payroll Office, comes under the total protection and responsibility of the staff and management of that office. It therefore behooves staff and management to know and understand the restrictions on disclosure of confidential information delineated in the California Information Practices Act (1977). Precautions to ensure that all necessary physical security interventions have been implemented is imperative to avoid inadvertent access or disclosure to unauthorized individuals. Any failure in this area could result in violations in which individuals, staff and/or management may be held liable. The SCO has no responsibility or control over the physical security controls of the department/campus.

Each individual must be aware of the potential disclosure of confidential data either through unlawful use of a password, unattended active terminal/PC, or inadvertent disclosure. The latter problem is usually the result of unauthorized individuals viewing confidential data via a screen or documents left out on a desk. Regardless of the manner of exposure, the individual controlling the documents and/or the physical security of the office is responsible for the violation and any subsequent legal consequences as a result of the disclosure. Therefore, all hard copies (including printouts) of data extracted from the SCO systems remain confidential, and are to be protected by department/campus personnel from unauthorized disclosure as stipulated in the California Information Practices Act (1977).

The Office of the State Controller adheres to the regulations and requirements set forth in the California Information Practices Act (1977) as well as the Federal Privacy Act (1974). Each department/campus staff member accessing confidential personal data is encouraged to read and follow the tenets of both these state and federal statute.