ACCESS TO THE STATE CONTROLLER'S OFFICE DATABASE/DOCUMENT PROCESSING 1165

(No. 109 May 2006)

Personnel employees shall consider all information residing in the State Controller's Office (SCO) database as sensitive and confidential. Access to information provided through the SCO system is restricted to authorized personnel only. SCO maintains several automated security control systems. Accidental or intentional misuse or disclosure of information by unauthorized or authorized users may result in disciplinary or punitive action. To reduce this risk, it is necessary for the Department to establish and enforce these requirements for all SCO system users.

REFERENCE(S) 1165.1

(No. 109 May 2006)

California Penal Code Section 502
California Information Practices Act - 1977

GENERAL PROVISIONS OR POLICY 1165.2

(No. 109 May 2006)

It is the policy of the California Department of Forestry and Fire Protection (CDF) to maintain secure and authorized access to the SCO Personnel/Payroll System. SCO maintains a dedicated computer that houses numerous systems of records, which contain confidential and sensitive data. Although automation provides valuable information, access to centrally stored machine readable data increases the risk of unwarranted disclosure or misuse of this data. Therefore, the SCO restricts such access to those individuals who have a bonafide need and legal justification for such access.

CRITERIA 1165.3

(No. 109 May 2006)

Access is granted to an individual based on four factors:

1. He or she must have access to confidential personnel/payroll data in order to perform legal, statutory, government duties;
2. He or she must be a bonafide employee of the State and, specifically, of the requesting department;
3. He or she must complete and sign a Security Authorization Form (PSD 125A). This form must be signed/approved by the Department's Security Monitor and authorized manager; AND
4. He or she must complete and sign a Statement of Understanding (PSD 108).

Once access is approved, the authorized user is provided with a UserID and password. The authorized user MUST protect his/her password at all times. The UserID and password should never be disclosed or shared with anyone. Failure to protect a UserID and password may result in a 30-day suspension from access to the SCO system. Further failure to protect the password may result in permanent cancellation of access. These actions are not to be misconstrued as punitive; rather, they are merely corrective actions and safety precautions to limit further misuse of the SCO system.

Once an authorized user logs on to the SCO system, any and all transactions or data keyed in under that UserID and password belongs to that individual regardless of the circumstances or the legality of the information entered. The liability, however, for any illegal transactions belongs to the authorized user (owner) of the password, not the person who entered the transaction. Therefore, each authorized user must log off (deactivate a session) prior to leaving a terminal or personal computer.

The responsibility for protecting confidential and sensitive data residing on the SCO system is a shared effort. SCO has a limited role in the total security effort. SCO's responsibility encompasses the area of data, telecommunications, and access security. Access security at the initial point is dependent on Department management selecting and requesting access for an individual who meets the criteria. SCO may investigate, if necessary, an individual who does not appear to meet the criteria.

The area that is not so easily understood is the level of protection of confidential data that is either viewable on individual video monitors, extracted from a printer, or keyed into the SCO system. This data, once it is removed, viewed, or processed into the SCO system comes under the total protection and responsibility of the staff and management of that office. Therefore, it is critical that staff and management know and understand the restrictions in the California Information Practices Act. Precautions to ensure that all necessary physical security interventions have been implemented are imperative to avoid inadvertent access or disclosure to unauthorized users. Any failure in this area may also result in punitive or disciplinary action. SCO has no responsibility or control over the physical security area of the department.

Each authorized user must be aware and cognizant of the potential disclosure or misuse of confidential data stored in the SCO system either through unlawful use of the UserID and/or password, an unattended active terminal, or a personal computer. No matter the violation, the authorized user controlling the documents and/or the physical security of the office is responsible for any violation or misuse of the SCO system.

PROCEDURES 1165.4

(No. 109 May 2006)

Authorized users of the SCO system shall not process and/or key personnel related documents that affect their own personnel and payroll history. Personnel and payroll documents for personnel specialists will be processed as follows:

Units:

1 person office:	Send all personnel and payroll documents to the Region Personnel Administrative Officer for processing.
2 person office:	All personnel and payroll documents must be processed by the counterpart.
Region Offices:	All personnel and payroll documents must be processed bya counterpart.
Sacramento Headquarters:	All personnel and payroll documents are processed by the personnel specialist responsible for the Human Resources assignment. The personnel and payroll documents for the Human Resources personnel specialist are processed by a counterpart.

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)