

CALIFORNIA
STATE CONTROLLER'S OFFICE
PERSONNEL / PAYROLL SERVICES DIVISION

DECENTRALIZED SECURITY PROGRAM MANUAL



REVISED DECEMBER 2015

NOTICE

The State Controller's Office (SCO) is in compliance with the requirements and restrictions of the California Information Practices Act of 1977. These guidelines are provided to help departments and campuses avail themselves of the many automated applications of the Personnel/Payroll system within SCO. However, these guidelines are not intended to encompass all the laws that may be applicable or impact each department or campus.

For specific information, please consult the California Civil Code, Division 3, Part 4; Title 1.8., Personal Data, Chapter 1, Information Practices Act of 1977 or the Information Practices Act Officer for your department/campus.

As it becomes necessary, the information in this document may be changed or updated to meet the needs of the Personnel/Payroll Services Program.

If the department/campus Security Monitor or Authorizing Official/Manager changes please follow the instructions in this manual under: Security Monitor Designation Procedures.

Copies of this document may be obtained from:

STATE CONTROLLER'S OFFICE
Personnel/Payroll Services Division
PO Box 942850
Sacramento, CA 94250-5878
ATTN: Decentralized Security Administrator

Table of Contents

INTRODUCTION	5
OBJECTIVES	5
REGULATORY BACKGROUND	5
Article 1 - General Provisions and Legislative Findings	5
Article 2 – Definitions.....	5
Article 5 - Agency Requirements	5
Article 6 - Conditions of Disclosure	5
STATE ADMINISTRATIVE MANUAL	6
§5300.4 - Definitions	6
§5300 - §5365.3 - Responsibilities of Users of Information.....	6
INFORMATION SECURITY.....	7
Confidentiality of SCO/PPSD Information	7
Computer Storage of Information	7
ORGANIZATIONAL RESPONSIBILITIES	7
State Controller’s Office	7
Personnel/Payroll Services Division.....	7
Decentralized Security Administrator	8
Civil Service Departments/Campuses	8
Authorizing Official/Manager	9
Security Monitor	10
Assistant Security Monitor.....	11
Alternate Security Monitor	11
SECURITY MONITOR DESIGNATION PROCEDURES.....	12
ACCESS REQUIREMENTS	13
Letter of Justification	14
User IDs	14
Passwords - Selection and Protection.....	15
Forgot Your Password?.....	15
Requesting System Access Procedures	16
Revocation and Deletion of User IDs	17
Security Authorization Form, PSD125A - Completion Instructions.....	17
Adding a New User	18

Adding a New User (Cont)	19
Change or Delete	20
EQUIPMENT AND SYSTEM CHANGES	21
AUTOMATIC SECURITY ACCESS DELETION	21
SECURITY VIOLATIONS	21
SECURITY AWARENESS	22
DECENTRALIZED SECURITY ADMINISTRATOR SITE VISITS	22
ANNUAL SELF-CERTIFICATION	23
NEED HELP?	24
DECENTRALIZED SECURITY GUIDELINES	25
Background	26
Controlling Access to Confidential Data	27
Controlling Access to Confidential Data (Cont)	28
Responsibility for Protecting Confidential Data	29
PSD125A	30

DECENTRALIZED SECURITY FORM LINKS

PSD040 - http://www.sco.ca.gov/Files-PPSD/PSD040_Security_Designee.pdf

PSD041 - http://www.sco.ca.gov/Files-PPSD/PSD041_Statement_of_Self-Certification.pdf

PSD108 - http://www.sco.ca.gov/Files-PPSD/PSD108_Statement_of_Understanding.pdf

INTRODUCTION

The purpose of this manual is to define the State Controller's Office (SCO) security requirements for all decentralized users of the Personnel/Payroll Services Division (PPSD) systems. SCO allows access to individuals who have an authorized, legal, and legitimate business need to access such data in the performance of their governmental duties.

Careless, accidental, or intentional disclosure of information to unauthorized persons can have detrimental effects, which may result in civil or criminal actions against those involved in unauthorized disclosure (please refer to [California Penal Code 502](#) and the [California Information Practices Act of 1977 \(IPA\)](#)). To reduce the risk of exposure, PPSD has established the necessary standards, procedures, practices, and controls to protect information resources against accidental or intentional disclosure, destruction or modification. This manual is designed to enhance rather than replace existing laws, rules and standards.

OBJECTIVES

The overall objective of this manual is to document the requirements that allow all affected parties to understand their responsibilities. These responsibilities include the following:

- Secure, maintain, and monitor the confidentiality and integrity of SCO's sensitive and confidential data.
- Protect SCO's data and systems against misuse, abuse, and unauthorized use.

REGULATORY BACKGROUND

To ensure current applicability to your department/campus specific needs, please review the [IPA](#) and [SAM](#) or contact your department/campus IPA Officer and/or Information Security Officer.

Article 1 - General Provisions and Legislative Findings

[§1798 - §1798.1](#)

Article 2 – Definitions

[§1798.3](#)

Article 5 - Agency Requirements

[§1798.20 - §1798.21](#)

Article 6 - Conditions of Disclosure

[§1798.24](#)

STATE ADMINISTRATIVE MANUAL

§5300.4 - Definitions

- Confidential Information:
- Custodian of Information:
- Information Assets:
- Information Security:
- Owner of Information:
- Physical Security:
- Privacy:
- Public Information:
- Sensitive Information:
- User Information:

§5300 - §5365.3 - Responsibilities of Users of Information

INFORMATION SECURITY

Confidentiality of SCO/PPSD Information

All information residing on SCO's systems is considered to be sensitive/confidential and must be treated as such by all persons who are granted access. Therefore, this information must be protected from unauthorized access or disclosure.

- All hard copies (including printouts) of data produced from PPSD's systems are considered confidential and must be processed/destroyed accordingly.

NOTE: Standard email, instant messaging and file transfer services are not secured services and therefore the transmission of confidential/sensitive data including social security numbers via these services is prohibited.

Computer Storage of Information

Decentralized departments/campuses are prohibited from storing confidential/sensitive SCO information on any computer system, including microcomputers, which is not under SCO's direct control unless authorized on a case by case basis by SCO's Chief Information Security Officer and PPSD Decentralized Security Administrator.

ORGANIZATIONAL RESPONSIBILITIES

State Controller's Office

The SCO is responsible for numerous statewide programs that handle confidential and sensitive data resulting in the annual disbursement of tens of billions of dollars each fiscal year. Due to the number, size, and complexity of these statewide programs, the proliferation of alternative automated processing capabilities and legislation relating to data confidentiality and security requirements, SCO has developed a centralized approach to addressing security needs of the decentralized departments/campuses.

Personnel/Payroll Services Division

PPSD is responsible for the integrity and maintenance of the Employment History (PIMS) and Payroll History (HIST) databases, as well as the Affordable Care Act Database (ACAS). PPSD also has application files allowing the decentralized departments/campuses to update those files and issue various types of pay through the Payroll Input Process (PIP), maintain Leave Accounting Records (LAS), view the on-line Civil Services Pascale (CSP), perform Master Payroll Certification (MPC) and design Ad-Hoc Reports through the Management Information Retrieval System (MIRS).

Decentralized Security Administrator (DSA)

The Decentralized Security Administrator acts on behalf of PPSD for the various applications used in the decentralized environment. The Decentralized Security Administrator also manages the PPSD Decentralized Security Program, serves as SCO's liaison with all decentralized civil service department/campus Security Monitors and is required to ensure compliance of all SCO security procedures as identified by SCO's Information Security Manual Program Standards Manual.

Responsibilities:

- Conducts audits of departments/campuses to ensure all required forms and justifications are up to date. These audits may be conducted at any time at the discretion of PPSD.
- Ensures the implementation, enhancement, monitoring, and enforcement of the Decentralized Security Program.
- Provides direction and leadership of the security program through the development of standards and ensures compliance with these standards.
- Approves/disapproves requests from civil service departments/campuses for personnel/payroll system application access to the PPSD systems.
- Authorizes and coordinates activation of equipment (terminals, printers) to the SCO Network.
- Authenticates all alleged decentralized security violations and takes appropriate corrective action.
- Represents the SCO in all decentralized security matters.
- Coordinates and directs decentralized security program activities and reporting processes.

Civil Service Departments/Campuses

Each department/campus is responsible for protecting PPSD's confidential and sensitive data. This requires the designation of a Security Monitor who is responsible for compliance with the security program requirements, and is designated as the contact person to whom PPSD will address all security matters. The individual selected must take responsibility for the system users within their department/campus and have the necessary authority to complete duties specified in this manual. Departments/campuses must report any variances from established procedures to the PPSD Decentralized Security Administrator. Department/campuses will adhere to Civil Code Section [1798.14-1798.23](#).

Authorizing Official/Manager

The Authorizing Official/Manager is typically the Personnel or Payroll Officer/Manager. However, each department/campus may vary in its control and authority levels of management. The Authorizing Official/Manager must be the one who is responsible for the personnel/payroll functions in each department/campus.

Responsibilities:

- Ensures compliance with the standards and procedures in this manual, which includes providing PPSD with the following documents:
- Submits the Annual Statement of Self Certification form, PSD041 by January 31st of each year on behalf of the department/campus.
- Submits written justification(s) for user access when applicable.
- Requests equipment and system changes as needed.
- Submits a Security Authorization Form (PSD125A) on behalf of the department/campus.
- Submits Statement of Understanding form (PSD108) on behalf of the department/campus.
- Verifies access and level of access of existing staff listed on the PSD125A. Once an employee changes to another classification, a new PSD108 is required advising PPSD of the change in classification (provide a justification if necessary).

NOTE: An individual with access to the PPSD system and who is listed on the PSD125A cannot be the signature for the Authorizing Official/Manager.

- Designates a Security Monitor on the Security Monitor Designee form, (PSD040).
- Approves and signs the Security Authorization form (PSD125A),
- Protects the confidentiality of SCO/PPSD data and maintain appropriate physical security as mandated in the [IPA](#) and the [SAM](#).

NOTE: Signing the Security Authorization form (PSD125A) authorizes and stipulates that individual(s) named on the document are bona fide employees of the department/campus and must have access to the applications and/or role(s) enumerated on the form in order to perform the official governmental or statutory duties of their position as mandated in the [IPA](#).

It is required that verification be made of users listed on the PSD125A to ensure access and level of access is appropriate prior to signing the PSD125A. Signature is confirmation and acceptance of this responsibility and authorization.

Security Monitor

PPSD requires each department/campus to designate a responsible individual as a Security Monitor. The Security Monitor must have a working knowledge of the PPSD systems and applications, and the types of data they contain as well as the different levels of system access.

Responsibilities:

- Ensures compliance with the standards and procedures in this manual.
- Acts as the departmental liaison to the PPSD Decentralized Security Administrator.
- Acts as the security resource for all departmental personnel/payroll office staff as it relates to SCO security requirements.
- Maintains the Decentralized Security Program Manual and current Security Authorization forms.

Security Authorization Forms:

- [PSD108 - STATEMENT OF UNDERSTANDING](#)
- [PSD040 – SECURITY MONITOR DESIGNEE](#)
- [PSD041 – ANNUAL STATEMENT OF SELF-CERTIFICATION](#)
- PSD125A - SECURITY AUTHORIZATION (SEE PAGE 30 BELOW)
- Retains the PSD125A and PSD108 for five years after the date of last access for any user that is no longer active at that department/campus.
- Submits the Security Authorization form – PSD125A:
 - ADDS – Lists new users on current PSD125A; include appropriate attachments.
 - DELETES – See "Revocation and Deletion of User IDs"
 - CHANGES – Additional access, reduction in access, name changes, leave of absence.
- Verifies access and level of access of existing staff listed on the PSD125A. Once an employee changes to another classification or has a name change, a new PSD108 is required advising PPSD of the change, and a justification if necessary.

By signing the PSD125A, the Security Monitor is certifying that all appropriate security forms are completed and attached.

- Reviews turnaround on PSD125A for changes.
- Trains new authorized users on logon procedures into PPSD systems.
- Immediately reports all security infractions and violations to the PPSD Decentralized Security Administrator.

Assistant Security Monitor

An Assistant Security Monitor is normally considered for each area that is not physically located near the designated Security Monitor. For example, some departments/campuses have exam units not located within the personnel office and some campuses have personnel offices not located within the payroll office. Each Assistant Security Monitor must ensure compliance with the standards and procedures spelled out in this manual for their respective area and in overall support of the Security Monitor.

Alternate Security Monitor

Due to the size and complexity of some departments/campuses it may be necessary to establish an Alternate Security Monitor to act on behalf of the Security Monitor in his/her absence. The Alternate Security Monitor must perform the responsibilities of the Security Monitor. The same designation procedures apply as for the Security Monitor.

SECURITY MONITOR DESIGNATION PROCEDURES

- Selection of a Security Monitor is made by the Personnel/Payroll Officer or higher appropriate level of management.
- Selection Criteria (refer to "Security Monitor Responsibilities") - the designee must be selected on the basis of their ability to fulfill the responsibilities of the position as indicated. The individual must work within the Personnel/Payroll Office and have the authority to carry out the duties specified in this manual.
- The Security Monitor Designee form, PSD040, must be completed and signed.

NOTE: The signatures of the Security Monitor and the Authorizing Official on the Security Monitor Designee form, PSD040, are the only signatures accepted on the Security Authorization form, PSD125A. If these signatures do not match, the PSD125A will be returned.

Should a change in the Authorizing Official or Security Monitor occur, a new Security Monitor Designee form, PSD040, is required. If a blank Security Monitor Designee form, PSD040, is not available, you may obtain one by contacting the Decentralized Security Administrator at:

STATE CONTROLLER'S OFFICE
Personnel/Payroll Services Division
P.O. Box 942850
Sacramento, CA 94250-5878
ATTN: Decentralized Security Administrator
Or
Email: dsa@sco.ca.gov

NOTE: The PPSD Decentralized Security Administrator maintains a file of current Security Monitors. This information is provided to the SCO's Information Security Officer once a month.

ACCESS REQUIREMENTS

Access and use of the SCO's Human Resource Management systems shall only be initiated from workstations that are owned or leased by the state agency and that are physically located within a facility that is owned or leased by the state agency.

Access to information available through the PPSD system is restricted to AUTHORIZED PERSONS ONLY. Any person requesting such access **MUST** meet the following criteria:

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

The PPSD system contains sensitive and confidential information. Access is restricted to persons with an authorized, legal, and legitimate business requirement to complete their duties.

Department Wide access to PIMS and HIST is only given to departments headquarters office that have more than one location and the need for Personnel and Payroll capabilities. Access is inquiry only and will only be reviewed and approved on a case by case basis.

Currently, PIMS, HIST, KEYM, PIP, LAS, MPC and/or ACAS applications are restricted to Personnel Specialists or Personnel Technician classifications because their need is by definition a function of their specific job duties and any change in those duties requires a reevaluation of the need for access.

If the employee's duties change, such that the need for access no longer exists, the access privilege **MUST** be removed or deleted immediately by a request submitted by the department/campus.

Letter of Justification

A request to grant access to an individual in a classification other than in the Personnel Specialist/Payroll Technician series to access PIMS, HIST, KEYM, PIP, LAS, MPC and/or ACAS requires a written justification from the Authorizing Manager. The justification must describe the individual's specific job duties requiring the need to access system information (i.e., **PIMS** = Employment History, **HIST**=Payroll History, **LAS**=Leave Accounting System, etc.) as well as level of access to that application, in order to perform their regular daily duties. **Manager classifications will be granted inquiry access only.**

- A request to grant access to an individual in an out of class assignment requires a justification. The justification must include the time table of the out of class assignment.
- In order for the user to be allowed access, the PPSD Decentralized Security Administrator must establish that the user needs the access to perform his/her regular daily duties.
- Access is denied/revoked if it is determined that the application the user is requesting is not part of his/her regular daily duties.

User IDs

Each individual who is approved by the Decentralized Security Administrator to access the PPSD systems is provided with a unique "User ID".

The SCO's Information Security Office builds the user ID and connects it to the approved application(s). When completed they will contact the Security Monitor and release both the user ID and a generic password. The Security Monitor will then assist the user to log into PPSD system and verify all requested access is functional. When the user logs on for the first time using the generic password, the system will prompt him/her to enter a new password.

If a user will be on an extended leave of absence (LOA), notify the PPSD Decentralized Security Administrator immediately with the users name, user id and time frame so the user id can be locked temporarily and not deleted. When the user returns to work and notify the PPSD Decentralized Security Administrator to reactivate. Contact the PPSD Decentralized Security Administrator at dsa@sco.ca.gov.

Passwords - Selection and Protection

Access is restricted to authorized persons through the use of passwords. Each User ID requires a password known only to its owner.

The requirements for selecting a password are:

- Must be eight characters
- Must contain one uppercase alphabetic character
- Must contain one lowercase alphabetic character
- Must contain one numeric character

Passwords must be changed every ninety (90) days. Avoid using an obvious password such as individual's nickname or other easily identifiable password.

For self-protection, the password owner must:

- Not reveal/share their password to ANYONE.
- Not write down the password.
- Not log on to provide access/use by anyone.
- Always lock terminal or log off before leaving workstation.

If a user has been given a new/temporary password he/she has 30 days to logon to the system and activate the account, if not, his/her access will be deleted.

Forgot Your Password?

Contact the SCO Information Security Office at (916) 322-8094. They will validate the owner's identity and give a generic password.

Requesting System Access Procedures

To request system access, each department/campus Security Monitor must perform the following:

- Have the department/campus employee user read the Security Guidelines package and sign the Statement of Understanding form, PSD108. The employee is to retain the information portion of the package and provide the original signed PSD108 to the Security Monitor.
- The PSD108 MUST be completed by each employee who requests system access.
- Ensure all access requests are in writing, using the most current Security Authorization form, PSD125A.
- Ensure all pages of the PSD125A and any PSD108 forms are routed together to the Decentralized Security Administrator via the Security Monitor of the requesting department/campus.
- The Decentralized Security Administrator will validate the accuracy of all requests and approve/disapprove requests for access to the PPSD systems. The PSD125A is then sent to the SCO Information Security Office for final processing.
- Once access is approved/disapproved and processed a current PSD125A is sent to the department/campus Security Monitor. The PSD125A is then reviewed for accuracy and retained for future use. Contact the Decentralized Security Administrator for any discrepancies.

Revocation and Deletion of User IDs

To prevent unauthorized use by a transferred, terminated or resigned employee's user ID, the Security Monitor must IMMEDIATELY submit all pages of the PSD125A to delete the user's system access. Using an old user ID increases the chances of a security breach which is a serious security violation. Sharing a user ID is strictly prohibited and a serious violation.

If a user ID is inactive for 90 days it is assumed that access is no longer required. User IDs may be revoked without notice if they are not used regularly.

Security Authorization Form, PSD125A - Completion Instructions

When a department/campus or PPSD initiates any type of change on the PSD125A, a revised PSD125A is mailed once the changes have been completed. Please verify for accuracy once the revised PSD125A is received.

If you do not receive a revised copy of your departments PSD125A contact the decentralized security administrator at dsa@sco.ca.gov.

Forms should be sent to:

STATE CONTROLLER'S OFFICE
Personnel/Payroll Services Division
P.O. Box 942850
Sacramento, CA 94250-5878
ATTN: Decentralized Security Administrator

Adding a New User

Each employee who requires access to the PPSD systems must read the Decentralized Security Guidelines and sign the Statement of Understanding form, PSD108. This form is required when submitted with form PSD125A, as a package.

To request access for a new user, the columns on the PSD125A are completed as followed below:

COLUM	EXPLANATION
NAME	Enter employee's last name, first name, and middle initial as it appears on the Employment History data base.
USER ID	Leave Blank. For SCO USE ONLY. Make no entry.
CLASS 4-DIGIT (CLASSIFICATION)	Indicate 4-digit class code
TC (TYPE OF CHANGE)	Indicates Type of Action requested. A = Add, C = Change, D = Delete. Enter "A" to add a new user.
APPLICATIONS:	NOTE: There are various levels of access for the PIMS and LAS applications:
PIMS = EMPLOYMENT HISTORY	Enter "I" if employee will "Inquire" only. Enter "O" if employee will "Inquire", "Update", and key "Out-of-Sequence" documents.
HIST = PAYROLL HISTORY	Enter "X" under the application name(s) required for the employee.
KEYM = KEYMASTER - BATCH PROCESS	Enter "X" under the application name(s) required for the employee.
PIP = PAYROLL INPUT PROCESSING	Enter "X" under the application name(s) required for the employee.
MIRS = MANAGEMENT INFORMATION RETRIEVAL SYSTEM	Enter "X" under the application name(s) required for the employee.
DWPIMS= DEPARTMENTWIDE PIMS	Enter "X" under the application name(s) required for the employee.

Adding a New User (Cont)

COLUMN	EXPLANATION
DWHIST = DEPARTMENTWIDE HIST	Enter "X" under the application name(s) required for the employee.
CSP = CIVIL SERVICE PAYSCALES	Enter "X" under the application name(s) required for the employee.
LAS = LEAVE ACCOUNTING SYSTEM	Enter "I" if employee will "Inquire" only. Enter "U" if employee will "Inquire" and "Update".
MPC = MASTER PAYROLL CERTIFICATION	Enter "X" under the application name(s) required for the employee
VIEW = VIEWDIRECT	Enter "X" under the application name(s) required for the employee.
IDLS = IDL CALCULATOR	Enter "X" under the application name(s) required for the employee
ACAS = AFFORDABLE CARE ACT DATABASE	Enter "I" if employee will "Inquire" only. Enter "U" if employee will "Inquire" & "Update".
REMARKS	Make any remarks or comments that are applicable
AUTHORIZING OFFICIAL/MANAGER'S SIGNATURE	Legal signature and working title of the individual accepting responsibility for all employees listed, and date signed. This individual cannot be a system user and must be the certifying official identified on the Security Monitor Designee form, PSD040. Each page must be signed.
SECURITY MONITOR'S SIGNATURE	Legal signature of the individual who is designated as the Department/campus Security Monitor, Assistant Security Monitor or Alternate Security Monitor. Each page must be signed.

Change or Delete

To change/delete user information on the PSD125A due to a separation, transfer, change in classification, name change, or change in duties, the change/delete must be documented on PSD125A and SCO notified immediately.

Complete a "Change" or "Delete" as follows:

COLUMN	EXPLANATION
NAME	Enter an asterisk (*) after the appropriate name to identify the user.
TC	Enter "C" if requesting a change to user information. Enter "D" if requesting to delete a user.
REMARKS	Enter a brief description of the change desired, and a reason for the change or delete.
SIGNATURES	Refer to signature instructions shown above.

EQUIPMENT AND SYSTEM CHANGES

(Adding new/additional equipment)

Any requests for equipment connection and access (i.e. terminals, printers, personal computers, etc.) into the SCO's systems must be made in writing by the Personnel/Payroll Manager, Security Monitor or appropriate higher level management and submitted to the Decentralized Security Administrator. Once the Decentralized Security Administrator acknowledges the request, the Decentralized Security Administrator will then provide the department/campus the SCO Decentralized Customer Information Security Statement of Understanding and Compliance Validation documents (known as the Teleprocessing Security Requirements). These documents must be completed by the requesting department/campus Information Technology staff, and then returned to the Decentralized Security Administrator

AUTOMATIC SECURITY ACCESS DELETION

The SCO conducts a quarterly security audit that identifies individuals who have not used the system for 90 consecutive days and automatically deletes them from the system.

Reinstatement access for an individual who was automatically deleted requires a new justification signed by the authorizing manager regarding the non-use and reinstatement, along with the PSD 125A and a new PSD 108.

SECURITY VIOLATIONS

It is the responsibility of all users to protect SCO resources, to note variances from established procedures, and to report such variances to their Security Monitor who shall report them to the SCO Decentralized Security Administrator.

During the time when a suspected violation is under investigation, the suspected violator's access privileges may be revoked and/or other action may be taken to prevent further potential harm to SCO assets.

All violations of security standards and/or procedures are subject to disciplinary action. The specific disciplinary action that will be taken depends upon the nature of the violation, the impact of the violation to SCO's informational assets and related facilities, etc.

If applicable to the entity, the provisions of [SAM 5340](#) and [SIMM 5300 - 5340-A](#) should be observed regarding information security incident reporting.

SECURITY AWARENESS

Each decentralized user who is authorized access to PPSD systems must review the Decentralized Security guidelines annually. All departments/campuses must provide copies of the guidelines to each employee in their personnel/payroll offices.

This ensures that all system users are consciously aware of their responsibilities for preserving and protecting PPSD systems. Contact the Decentralized Security Administrator at dsa@sco.ca.gov for a copy of the guidelines if needed.

DECENTRALIZED SECURITY ADMINISTRATOR SITE VISITS

The Decentralized Security Administrator will set appointments for site and security information visits with department/campus representatives (including organizational Security Monitors, Personnel Offices, Divisional and Departmental Management). The purpose of these site visits is to discuss measures and interventions for protecting sensitive confidential data, and will include the following:

- Ensures Security measures are in place.
- Meets Security Monitors and Authorizing Managers.
- Gains a better understanding of the sections/units within the departments that access the SCO systems.
- Answers questions on forms (PSD125A, PSD108, PSD040 and PSD041).

ANNUAL SELF-CERTIFICATION

All PPSD decentralized departments/campuses are responsible to annually certify that they are in compliance with the Security Program standards. The Security Monitor and appropriate level managers should review the Decentralized Security Program Manual and apply the standards and procedures to their respective decentralized site, as well as review the Decentralized Security Guidelines once a year with staff.

The Annual Statement of Self Certification form, PSD041, is due to the Decentralized Security Administrator by January 31st of each year. To ensure compliance, a copy of this completed form must be maintained by the department/campus for future reference.

If the decentralized department/campus is not in compliance, a letter explaining the deficiencies and a corrective action plan is sent to the Decentralized Security Administrator by January 31st of each year.

Annual Statements of Self-Certification not received by January 31st of each year are considered in non-compliance of the PPSD Decentralized Security Program and Guidelines and the [IPA](#).

If the Authorizing Manager separates at any time during the year, a newly appointed Authorizing Manager must complete and resubmit the PSD041.

NOTE: Failure to provide the Annual Statement of Self-Certification by January 31st of each year will result in the revocation of access for all office staff and deactivation of all personnel/payroll data equipment to the SCO systems.

NEED HELP?

For those departments/campuses that access the SCO network via personal computers it is recommended that you first contact your Information Technology staff when having problems with hardware/software or any other equipment problems.

The following is a list of help desk contacts:

Department	Contact Number
Office of Technology Services (OTECH)	Help Desk (916) 464-4311 Service.desk@state.ca.gov
SCO's Information Security Office	Help Desk (916) 322-8094

DECENTRALIZED SECURITY GUIDELINES

CALIFORNIA
STATE CONTROLLER'S OFFICE



PERSONNEL / PAYROLL SERVICES DIVISION
PROGRAM

DECENTRALIZED SECURITY GUIDELINES

THIS PACKAGE MAY BE REPRODUCED TO PROVIDE INDIVIDUAL COPIES TO STAFF

REVISED SEPTEMBER 2015

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. Therefore, SCO restricts such access to those individuals who have a bona fide business need and legal justification for such access.

SCO maintains several automated security control systems, which will continue to be modified as needed, or when more sophisticated technology 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 and use of the SCO's Human Resource Management Systems shall only be initiated from workstations that are owned or leased by the state agency and that are physically located within a facility that is owned or leased by the state agency.

Access is granted to an individual based on four factors:

- Must have access to confidential Personnel/Payroll data in order to perform their legal, statutory, government duties. (If applicable, a "Justification Statement" must accompany this document if the individual does not have a classification that denotes their employment is within the Personnel/Payroll area).
- Must be a bona fide employee of the State and specifically of the requesting department/campus.
- Completion of PSD125A, Security Authorization form, signed by the department/campus security monitor and authorized manager, attesting to the above mentioned factors.

AND

- Completion of the "Statement of Understanding," PSD108, acknowledging that the individual has read and understands these guidelines.
- These factors are reviewed and access is granted by the Decentralized Security Administrator who represents the Chief, PPSD.
- Once access has been approved, the individual is assigned a "User ID".
- The Security Monitor will be contacted by the SCO Information Security Office 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 SCO 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/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 SCO 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.

Controlling Access to Confidential Data (Cont)

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, any and 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), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

Responsibility for Protecting Confidential Data

The responsibility for protecting confidential and sensitive data residing on the SCO computer 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. The SCO will then verify, and if necessary, require justification for an individual who does not appear to meet the criteria. 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/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 computer 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 statutes.

OFFICE OF THE STATE CONTROLLER - PERSONNEL/PAYROLL SERVICES DIVISION
P.O. BOX 942850, SACRAMENTO, CA 94250-5878

DEPT/CAMPUS-ID:

ROUTE TO: **DEPT NAME:**
DEPT ADDRESS:
ATTN:

CURRENT SECURITY AUTHORIZATION AS OF: **December 10, 2015**

APPLICATIONS																	
NAME ----- LAST, FIRST, MI	USER ID	CLASS 4-DIGIT	T C	P I M S	H I S T	K E Y M	P I P	M I R S	D W P I M S	D W H I S T	C S P	L A S	M P C	V I E W	I D L S	A C A S	REMARKS

RETAIN THIS COPY FOR YOUR RECORDS AND FUTURE REVISIONS

STATE CONTROLLER USE ONLY

As the duly appointed authority, I hereby accept responsibility for this authorization and certify that granting access to confidential employee data for the above named individuals is in accordance with their constitutional or statutory duties as mandated in the Information Practices Act.

SCO/PPSD SECURITY MONITOR APPROVAL (SIGNATURE) DATE

AUTHORIZATION - MANAGER (SIGNATURE) DATE

ISO OWNER/CUSTODIAN APPROVAL (SIGNATURE) DATE

ACKNOWLEDGEMENT - SECURITY MONITOR (SIGNATURE) DATE

PSD125A (REV. 01/15)