

State Controller's Office

Personnel and Payroll Services Division

Decentralized Security Program Manual

NOTICE

The State Controller's Office (SCO) is in compliance with the requirements and restrictions of the California Information Practices Act of 1977 (IPA). These guidelines are provided to help departments and campuses avail themselves of the many automated applications of the SCO system. 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, IPA of 1977 or the IPA 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 and Payroll Services Program.

If the department/campus Security Monitor/Assistant Security Monitor or Authorizing Official/Assistant Authorizing Official changes, please follow the instructions in this manual under Security Monitor/Assistant/Security Monitor.

Revised October 2020

Copies of this document may be obtained from:

State Controller's Office
Personnel and Payroll Services Division
PO Box 942850
Sacramento, CA 94250-5878
ATTN: Decentralized Security Administrator
DSA@sco.ca.gov

CHANGE LOG

This record shall be maintained throughout the life of the document. Each change and published update shall be recorded.

CHANGE / REVISION RECORD

Date	Page	Description of Change	Made By
02/10/2020	3, 14	Added DSA Hours Of Operation	DSA
06/01/2020	6	Deleted workstations that are owned or leased by the state agency	DSA
10/16/2020	2, 6, 7, 8, 9	Removed Computer Storage of Information Removed Letter of Justification Removed SSM I Classifications Removed CEA, IT, Labor Relations Removed Student Assistants, Seasonal Clerk Removed T&D, OOC	DSA

Table of Contents

Introduction	1
Objectives	1
Regulatory Background	1
IPA of 1977	1
State Administrative Manual (SAM)	1
Information Security	2
Confidentiality of SCO/PPSD Information	2
Organizational Responsibilities	2
State Controller’s Office	2
Personnel and Payroll Services Division	2
Decentralized Security Administrator (DSA)	2
Civil Service Departments/Campuses	3
Authorizing Official/Assistant Authorizing Official	3
Security Monitor/Assistant Security Monitor	4
Security Authorization Forms	5
Access Requirements	5
Leave of Absence (LOA)	6
Passwords - Selection and Protection	6
Forgot Your Password	6
Requesting System Access Procedures	7
Revocation and Deletion of User IDs	7
Security Authorization Form, PSD125A- Completion Instructions	7
Adding a New User	8
Change or Delete	9
Equipment Changes - Printers	10
Automatic Security Access Deletion	10
Security Violations	10
Security Awareness	11
Annual Self-Certification	11
Change of Physical Address	11
Need Help	12
Attachment A	13

Add New User Example	13
Change User Example	14
Delete User Example.....	15

Helpful Links

[California Penal Code 502](#)

[Information Privacy Act of 1977](#)

[State Administrative Manual Section 5300](#)

[PSD108-Statement of Understanding](#)

[PSD040-Security Monitor Designee](#)

[PSD041-Annual Statement of Self-Certification](#)

[State Information Management Manual \(SIMM\)](#)

[Payroll Procedures Manual \(PPM\)](#)

[California Department of Technology](#)

Introduction

The purpose of this manual is to define the State Controller's Office (SCO) security requirements for all decentralized users of the Personnel and Payroll Services Division (PPSD) SCO system. 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 IPA of 1977). 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 parties to understand their responsibilities. These responsibilities include the following:

- Secure, maintain, and monitor the confidentiality and integrity of SCO's system.
- Protect SCO 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.

IPA of 1977

Article 1 - General Provisions and Legislative Findings §1798– §1798.1

Article 2 - Definitions §1798.3

Article 5 - Agency Requirements §1798.14–§1798.23

Article 6 - Conditions of Disclosure §1798.24–§1798.24b

State Administrative Manual (SAM)

Responsibilities of Users of Information - §5300 –§5365.3

Definitions - §5300.4

- Confidential Information
- Physical Security
- Custodian of Information
- Privacy
- Information Assets
- Public Information
- Information Security

- Sensitive Information
- Owner of Information
- User Information

Information Security

Confidentiality of SCO/PPSD Information

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

- All hard copies (including printouts) of data produced from the SCO system 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.

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, the SCO has developed a centralized approach to addressing security needs of the decentralized departments/campuses.

Personnel and Payroll Services Division

PPSD processes payroll and leave accounting for state civil service and exempt employees, as well as state court, and California State University employees. PPSD provides information required to manage the personnel resources of the state and to properly account for salary and wage expenditures. Finally, PPSD provides data to the retirement systems necessary for calculation of employee retirement benefits and manages the state's automated travel expense claim system.

Decentralized Security Administrator (DSA)

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

NOTE: SCO DSA hours of operation are from 6:30-4:00 Monday thru Friday.

Responsibilities:

- 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 and payroll system application access to the SCO system.
- 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 their own confidential and sensitive data contained in PPSD's systems. This requires the designation of a Security Monitor/Assistant 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 DSA and adhere to Civil Code Section 1798.14–1798.23.

Authorizing Official/Assistant Authorizing Official

The Authorizing Official/Assistant Authorizing Official 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/Assistant Authorizing Official must be responsible for the personnel and payroll functions in each department/campus.

Responsibilities:

- Ensures compliance with the standards and procedures in this manual, which includes providing PPSD with the documents referenced below.
- Submits the PSD041 by January 31 of each year on behalf of the department/campus.
- Submits the PSD125A on behalf of the department/campus.
- Submits the PSD108 on behalf of the department/campus.
- Verifies access and level of access of existing staff listed on the PSD125A.
- When an employee has a name change, a new PSD108 is required advising PPSD of the change.

- Designates a Security Monitor/Assistant Security Monitor on the PSD040.

NOTE: Signing the 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 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 the access and level of access is appropriate prior to signing each page of the PSD125A.

Signature is confirmation and acceptance of this responsibility and authorization.

Security Monitor/Assistant Security Monitor

PPSD requires each department/campus to designate a responsible individual as a Security Monitor/Assistant Security Monitor. The Security Monitor/Assistant Security Monitor must have a working knowledge of the SCO system 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, which includes providing PPSD with the documents referenced below.
- Acts as the departmental liaison to DSA.
- Acts as the security resource for all departmental personnel and payroll office staff as it relates to SCO security requirements.
- Maintains the Decentralized Security Program Manual and current Security Authorization forms.
- 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 PSD125A.
- ADDS – Lists new users on the current PSD125A; include appropriate attachments.
- DELETES – See "Revocation and Deletion of User IDs"
- CHANGES – Additional access, reduction in access, name changes, leave of absence, return to work.
- Verifies access and level of access of existing staff listed on the PSD125A.
- When an employee has a name change, a new PSD108 is required advising PPSD of the change.
- Reviews all documents for accuracy prior to approval.

By signing the PSD125A, the Security Monitor/Assistant 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 SCO system.
- Immediately reports all security infractions and violations to the DSA.

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

Security Authorization Forms

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

Should a change in the Authorizing Official/Assistant Authorizing Official or Security Monitor/Assistant Security Monitor occur, a new, PSD040, is required. If the PSD040 is not available, you may obtain one by contacting the DSA or on our website.

https://www.sco.ca.gov/ppsd_state_hr.html

State Controller's Office

Personnel and Payroll Services Division
ATTN: DSA
P.O. Box 942850
Sacramento, CA 94250 5878
Email: dsa@sco.ca.gov

Access Requirements

Access to information available through the SCO 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 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 DSA.

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

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

Each individual approved by the DSA to access the SCO system is provided with a unique "User ID".

The SCO Information Security Office (ISO) creates the User ID so that departments/campus employees have the ability to access the SCO system. SCO ISO activates the User ID and connects the employees to the approved application(s). When completed they will contact the Security Monitor/ Assistant Security Monitor. and release both the User ID and temporary password. The Security Monitor will then assist the user to log into the SCO 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 them to enter a new password.

Leave of Absence (LOA)

If a user is on an extended LOA, the Security Monitor should notify the DSA **immediately** with the user's name, User ID, and the period of the LOA so the User ID can be temporarily deactivated. When the user returns to work, the Security Monitor should notify the DSA to reactivate the User ID. Contact the DSA at dsa@sco.ca.gov.

Passwords - Selection and Protection

Access is restricted to authorized persons using passwords. Each User ID requires a password known only to its owner.

The requirements for selecting a password are:

- The password must be at least 8 characters in length.
- Must contain one Uppercase Letter A-Z.
- Must contain one Lowercase Letter a-z.
- Must contain one numeric character 0-9.
- 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 ISO 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 PSD108. The employee is to retain the information portion of the package and provide the original signed PSD108 to the Security Monitor.
- Ensure all access requests are in writing, using the most current PSD125A.
- Ensure all pages are signed by both Security Monitor /Assistant Security Monitor and Authorizing Official/Assistant Authorizing Official of the PSD125A and any PSD108 forms are routed together to the DSA via the Security Monitor of the requesting department/campus.
- The DSA will validate the accuracy of all requests and approve requests for access to the SCO system. The PSD125A is sent to the SCO ISO for final processing.
- Once access is approved and processed, a current PSD125A is sent to the department/campus Security Monitor. The Security Monitor should then review the PSD125A for accuracy and retain for future use. Contact the DSA for any discrepancies.

NOTE: The PSD108 MUST be completed by each employee that requests system access.

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 contact DSA by email. The Security Monitor/Assistant Security Monitor must submit all pages of the PSD125A signed by both Security Monitor Assistant Security Monitor and Authorizing Official/Assistant Authorizing Official to delete the user's system access. Using an old User ID increases the risk of a security breach, which is a serious security violation. Sharing a User ID is strictly prohibited.

If a User ID is inactive for (90) days, it is assumed that access is no longer required. User IDs will 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 can be emailed via a Secure Enterprise File Transfer once the changes have been completed. Please verify for accuracy once the revised PSD125A is received.

- Submitting your PSD125A in hard copy form may delay processing; we strongly recommend requesting a Secure Enterprise File Transfer so that your request can be processed more efficiently and paperless.
- If you do not receive a revised copy of your department's PSD125A contact the DSA who will initiate the Secure Enterprise File Transfer and return the updated PSD125A reflecting any recent (A)dds, (C)hanges, and/or (D)eletes.

NOTE: Email DSA to request a Secure Enterprise File Transfer if you choose to submit your forms electronically.

If you choose not to submit electronically, the forms can be mailed to:

State Controller's Office
 Personnel and Payroll Services Division
 ATTN: DSA
 P.O. Box 942850
 Sacramento, CA 94250 5878

[Adding a New User](#)

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

PSD 125A column explanations:

Column	Explanation
Name	Enter employee's last name, first name, and middle initial as it appears on the Employment History database.
User ID	Leave Blank. For SCO USE ONLY. Make no entry.
TC (Type of Change)	Indicate Type of Action requested. Enter "A" to add a new user.
APPLICATIONS:	NOTE: There are various levels of access for PIMS, LAS, and ACAS 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 = Department Wide PIMS	Enter "X" under the application name(s) required for the employee.
DWHIST = Department Wide HIST	Enter "X" under the application name(s) required for the employee.
CSP = Civil Service Pay scales	Enter "X" under the application name(s) required for the employee.

Column	Explanation
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/Assistant Authorizing Official Signature	Legal signature (hand written, electronic, digital) of the individual who is designated as the Authorizing/Assistant Authorizing Official must sign and date each page of the PSD125A.
Security Monitor/Assistant Security Monitor	Legal signature (hand written, electronic, digital) of the individual who is designated as the Security/Assistant Security Monitor must sign and date each page of the PSD125A.

See Attachment A, Add New User Example.

Change or Delete

To change/delete user information on the PSD125A due to a separation, transfer, or change in name 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 (Type of Change)	Enter "C" if requesting a change to user information. Enter "D" if requesting to delete a user.
APPLICATIONS:	NOTE: There are various levels of access for PIMS, LAS, and ACAS applications.
Remarks	Enter a brief description of the change desired, and a reason for the change or delete.

Column	Explanation
Signatures	Refer to signature instructions shown above.
Name	Enter an asterisk (*) after the appropriate name to identify the user.

See Attachment A, Change and Delete User Example.

Equipment Changes - Printers

(Adding new/additional equipment)

When adding new or changing additional equipment (i.e., ViewDirect printers) you must contact DSA to advise DSA of the new Printer ID. In addition, contact DSA if any users need to be connected from the old Printer ID to the new Printer ID.

Automatic Security Access Deletion

The SCO ISO 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. A secure email of explanation and an updated PSD125A reflecting the deletion will be provided to the department/campus Security Monitor.

Reinstatement access for an individual who was automatically deleted requires a new PSD125A and PSD108.

NOTE: New users have 30 days to logon to the SCO system and activate their account. If not, the account's access will be deleted.

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 DSA.

- 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.
- 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, SIMM 5300, and SIMM 5340-A should be observed regarding information security incident reporting.

Security Awareness

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

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

Annual Self-Certification

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

- The PSD041 is due to the DSA by January 31 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 DSA by January 31 of each year.
- Annual Statements of Self Certification not received by January 31 of each year is considered in non-compliance of the PPSD Decentralized Security Program, Guidelines and the IPA.
- If the Authorizing Official/Assistant Authorizing Official separates at any time during the year, a newly appointed Authorizing Official/Assistant Authorizing Official must complete and resubmit the PSD041.

NOTE: Failure to provide the PSD041 form by January 31 of each year will result in the revocation of access for all office staff and deactivation of all personnel and payroll data equipment to the SCO system.

Change of Physical Address

Anytime a department/campus relocates, you must contact DSA immediately so that DSA can refer you to the System Activities Coordination & Support (SACS) unit for further assistance (PPM section C100 & C101).

Need Help

For those departments/campuses that access the SCO network via personal computers it is recommended that you first contact your IT 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) – Service Desk	(916) 464-4311
SCO ISO Help Desk Hours: 8:00am-5:00pm	(916) 322-8094
SCO DSA <ul style="list-style-type: none">Hours of operation: 6:30am-4:00pmMonday thru Friday	dsa@sco.ca.gov

Attachment A

Add New User Example

DEPT/CAMPUS-ID:

ROUTE TO: DEPT NAME:
DEPT ADDRESS:
ATTN:

CURRENT SECURITY AUTHORIZATION AS OF:

NAME ----- LAST, FIRST, MI	USER ID	CLASS 4-DIGIT	APPLICATIONS													REMARKS		
			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	
DOE, JOHN E		1303	A	O	X	X	X					X	U	X	X	X	U	

Change User Example

DEPT/CAMPUS-ID:

ROUTE TO: DEPT NAME:
DEPT ADDRESS:
ATTN:

CURRENT SECURITY AUTHORIZATION AS OF:

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
DOE, JOHN E		1303	C	Ø I	X	X	X				X	U	X	X	X	U	

Delete User Example

DEPT/CAMPUS-ID:

ROUTE TO: DEPT NAME:
DEPT ADDRESS:
ATTN:

CURRENT SECURITY AUTHORIZATION AS OF:

NAME ----- LAST, FIRST, MI	USER ID	CLASS 4-DIGIT	APPLICATIONS													REMARKS		
			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	
DOE, JOHN E		1303	D	O	X	X	X					X	U	X	X	X	U	