Personnel/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. These guidelines are provided to help departments and campuses avail themselves of the many automated applications of the SCO 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
# CHANGE LOG

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

## CHANGE / REVISION RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Page / Paragraph</th>
<th>Description of Change</th>
<th>Made By:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


# Table of Contents

**Introduction** ................................................................................................................................. 1  
Objectives ........................................................................................................................................ 1  

**Regulatory Background** .................................................................................................................. 1  
**California Information Practices Act of 1977 (IPA)** ................................................................. 1  
  - Article 1 - General Provisions and Legislative Findings §1798 - §1798.1 ............................. 1  
  - Article 2 - Definitions §1798.3 ........................................................................................................ 1  
  - Article 5 - Agency Requirements §1798.14 - §1798.23 ................................................................. 1  
  - Article 6 - Conditions of Disclosure §1798.24 - §1798.24b ......................................................... 1  

**State Administrative Manual** ........................................................................................................ 1  
  - Responsibilities of Users of Information - §5300 - §5365.3 ......................................................... 1  
  - Definitions - §5300.4 ......................................................................................................................... 1  

**Information Security** ...................................................................................................................... 2  
  - Confidentiality of SCO/PPSD Information ...................................................................................... 2  
  - Computer Storage of Information .................................................................................................. 2  

**Organizational Responsibilities** ..................................................................................................... 2  
  - State Controller’s Office .................................................................................................................. 2  
  - Personnel/Payroll Services Division ............................................................................................... 2  
  - Decentralized Security Administrator (DSA) ................................................................................ 2  
  - Civil Service Departments/Campuses ............................................................................................ 3  
    - Authorizing Official/Manager ...................................................................................................... 3  
    - Security Monitor ............................................................................................................................ 4  
    - Assistant Security Monitor .......................................................................................................... 5  
    - Alternate Security Monitor .......................................................................................................... 5  

**Security Authorization Forms** ...................................................................................................... 5  
  - PSD108 - Statement of Understanding .......................................................................................... 5  
  - PSD040 - Security Monitor Designee ............................................................................................... 5  
  - PSD041 - Annual Statement of Self-Certification ......................................................................... 5  
  - PSD125A - Security Authorization .................................................................................................. 5  

**Security Monitor Designation Procedures** ................................................................................... 5  
  - Access Requirements ...................................................................................................................... 6  
    - Letter of Justification ...................................................................................................................... 6  
    - Staff Services Manager Classifications ...................................................................................... 7  
    - Career Executive Assignment (CEA), Information Technology (IT), Labor Relations, Student  
      Assistant, and Seasonal Clerk Classifications ............................................................................. 7  

**User IDs** ......................................................................................................................................... 7  
  - Leave of Absence (LOA) ................................................................................................................ 8
Training and Development (T&D) ................................................................. 8
Out of Class Assignment (OOC) ................................................................. 8

Passwords - Selection and Protection ....................................................... 8
Revocation and Deletion of User IDs ......................................................... 9
Security Authorization Form, PSD125A- Completion Instructions ............... 9

Adding a New User ................................................................................... 10
Add New User Example ........................................................................... 11
Change or Delete ..................................................................................... 11
Delete User Example ............................................................................... 12

Equipment Changes - Printers ................................................................. 12
Automatic Security Access Deletion ......................................................... 12

Security Violations .................................................................................. 13
Security Awareness .................................................................................. 13

Annual Self-Certification ......................................................................... 13
Change of Physical Address .................................................................... 14
Need Help ................................................................................................. 14
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) 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 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.

California Information Practices Act of 1977 (IPA)

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

Responsibilities of Users of Information - §5300 - §5365.3
Definitions - §5300.4

Confidential Information
Custodian of Information
Information Assets
Information Security
Owner of Information

Physical Security
Privacy
Public Information
Sensitive Information
User Information
Information Security

Confidentiality of SCO/PPSD Information

All information residing on SCO system is considered 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 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.

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 DSA 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 Payscale (CSP), perform Master Payroll Certification (MPC), and design Ad Hoc Reports through the Management Information Retrieval System (MIRS).

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, 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 can 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 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 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 DSA Department/campuses and 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 documents referenced below.
- Submits the Annual Statement of Self Certification form (PSD041) by January 31 of each year on behalf of the department/campus.
- Submits signed 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).
- Approves and signs the Security Authorization form (PSD125A).
- Protects the confidentiality of SCO/PPSD data and maintains appropriate physical security as mandated in the IPA and the SAM.
- Reviews all documents and memo justifications for accuracy prior to approval.

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 each page of the PSD125A. Signature is confirmation and acceptance of this responsibility and authorization.

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

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 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.
- Acts as the departmental liaison to the PPSD DSA.
- Acts as the security resource for all departmental personnel/payroll office staff as it relates to SCO security requirements.
- 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, classification change, name changes, leave of absence, return to work.
- Verifies access and level of access of existing staff listed on the PSD125A.
- Once an employee promotes to another classification or has a name change, a new PSD108 is required advising PPSD of the change and a justification if necessary.
- Reviews all documents and memo justifications for accuracy prior to approval.
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 SCO system.
- Immediately reports all security infractions and violations to the PPSD DSA.

**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 Authorization Forms**

- PSD108 - Statement of Understanding
- PSD040 - Security Monitor Designee
- PSD041 - Annual Statement of Self-Certification
- PSD125A - Security Authorization

**Security Monitor Designation Procedures**

- The Human Resources Management is responsible for the selection of the Security Monitor.
- Selection Criteria (refer to "Security Monitor Responsibilities"): the designee must be selected based on 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 PSD040 is not available, you may obtain one by contacting the DSA.
Access Requirements

Access and use of the SCO’s 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 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 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 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. Access is inquiry only and will only be reviewed and approved on a case-by-case basis.

Currently, Mainframe Systems Overview (PIMS, HIST, KEYM, PIP, MIRS, CSP, LAS, MPC, VIEW, IDLS, 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 via 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 Mainframe Systems Overview (PIMS, HIST, KEYM, PIP, MIRS, CSP, LAS, MPC, VIEW, IDLS 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.

- The justification must include the timetable of the out of class assignment.
- In order for the user to be allowed access, the PPSD DSA 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.
- DSA may need to request additional documents such as Duty Statements, Org Charts, etc. to help determine if access is necessary.

### Staff Services Manager Classifications

Managerial classifications will be granted inquiry access only. All requests for access will be considered on a case-by-case basis, and approval is at the discretion of the DSA.

- To properly segregate duties, managers that approve transactions should not be able to key the transactions that they approve.
- It is for this reason that the Decentralized Security Program limits input access for personnel/payroll managers.
- The DSA must determine that the user in a Managerial classification or equivalent classification needs the access.
- MPC or PIP access for Managerial classifications is prohibited.
- It is highly recommended that individuals with keying access do not key their own transactions.

### Career Executive Assignment (CEA), Information Technology (IT), Labor Relations, Student Assistant, and Seasonal Clerk Classifications

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.

- Any requests received by the DSA to allow access for users in a CEA classification, IT classification, Labor Relations classification, Student Assistant classification, and/or Seasonal Clerk classification will be denied.
- DSA will direct you to contact your department's Security Monitor and/or Authorizing Official/Manager so you can work directly with them to obtain the information needed.

### User IDs

Each individual who is 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 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 him/her to enter a new password.

Leave of Absence (LOA)

If a user is on an extended LOA, notify the DSA immediately with the user’s name, User ID, and “To and From Dates” so the User ID can be locked temporarily and not deleted. When the user returns to work, notify the DSA to reactivate. Contact the DSA at dsa@sco.ca.gov.

Training and Development (T&D)

If a user is on a T&D, notify the DSA immediately with the user’s name, User ID, and “To and From Dates” of the T&D. In addition, you must provide a justification memo and PSD125A.

Out of Class Assignment (OOC)

If a user is on an OOC, notify the DSA immediately with the user’s name, User ID, and “To and From Dates” of the assignment. In addition, you must provide a justification memo and PSD125A.

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:
- 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 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 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.
- Ensure all access requests are in writing, using the most current Security Authorization form, PSD125A.
- Ensure all pages are signed by both Security Monitor and Authorizing Manager 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/disapprove requests for access to the SCO system. The PSD125A is then sent to the SCO ISO 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 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 submit all pages of the PSD125A signed by both Security Monitor and Authorizing Manager 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 will be emailed via a secure Electronic 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 Electronic Transfer file 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 at dsa@sco.ca.gov DSA will initiate the Secure Enterprise File Transfer and send to you the updated PSD125A that will reflect 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/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 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:

<table>
<thead>
<tr>
<th>Column</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter employee’s last name, first name, and middle initial as it appears on the Employment History database.</td>
</tr>
<tr>
<td>User ID</td>
<td>Leave Blank. For SCO USE ONLY. Make no entry.</td>
</tr>
<tr>
<td>Class 4-Digit (Classification)</td>
<td>Indicate 4-digit class code</td>
</tr>
<tr>
<td>TC (Type of Change)</td>
<td>Indicate Type of Action requested. Enter “A” to add a new user.</td>
</tr>
<tr>
<td>APPLICATIONS:</td>
<td>NOTE: There are various levels of access for PIMS, LAS, and ACAS applications.</td>
</tr>
<tr>
<td>PIMS = Employment History</td>
<td>Enter “I” if employee will “Inquire” only. Enter “O” if employee will “Inquire”, “Update”, and key “Out-of-Sequence” documents.</td>
</tr>
<tr>
<td>HIST = Payroll History</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>KEYM = Keymaster - Batch Process</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>PIP = Payroll Input Processing</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>MIRS = Management Information Retrieval System</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>DWPIMS = Department Wide PIMS</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>DWHIST= Department Wide HIST</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>CSP = Civil Service Payscales</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
<tr>
<td>LAS = Leave Accounting System</td>
<td>Enter “I” if employee will “Inquire” only. Enter “U” if employee will “Inquire” and “Update”.</td>
</tr>
<tr>
<td>MPC = Master Payroll Certification</td>
<td>Enter “X” under the application name(s) required for the employee.</td>
</tr>
</tbody>
</table>
**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.

### Add New User Example

<table>
<thead>
<tr>
<th>NAME</th>
<th>USER ID</th>
<th>CLASS 4-DIGIT</th>
<th>TC</th>
<th>PIMS</th>
<th>HIST</th>
<th>KEYM</th>
<th>PIPS</th>
<th>MIRS</th>
<th>DWPMS</th>
<th>DWPHIST</th>
<th>CSP</th>
<th>LAS</th>
<th>MPC</th>
<th>VIEW</th>
<th>IDLS</th>
<th>ACAS</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOE, JOHN E</td>
<td>1303</td>
<td>AOXXX</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter an asterisk (*) after the appropriate name to identify the user.</td>
</tr>
<tr>
<td>TC (Type of Change)</td>
<td>Enter &quot;C&quot; if requesting a change to user information. Enter &quot;D&quot; if requesting to delete a user.</td>
</tr>
<tr>
<td>APPLICATIONS:</td>
<td><strong>NOTE:</strong> There are various levels of access for PIMS, LAS, and ACAS applications.</td>
</tr>
</tbody>
</table>
**Remarks**
Enter a brief description of the change desired, and a reason for the change or delete.

**Signatures**
Refer to signature instructions shown above.

**Name**
Enter an asterisk (*) after the appropriate name to identify the user.

### Change User Example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LAST, FIRST, MI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOE, JOHN E</td>
<td>1303</td>
<td></td>
<td>C O</td>
<td>X X X</td>
<td>X X</td>
<td>X</td>
<td>U I</td>
<td>X X</td>
<td>X X X X X</td>
<td>X I X X X</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

### Delete User Example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LAST, FIRST, MI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOE, JOHN E</td>
<td>1303</td>
<td></td>
<td>D I</td>
<td>X X X</td>
<td>X X</td>
<td>X</td>
<td>I</td>
<td>X X</td>
<td>X X X X X</td>
<td>X I X X X</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

### 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 justification regarding the non-use and justification for reinstatement along with the PSD125A and a new 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 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, 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/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 Annual Statement of Self Certification form, 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 are considered in non-compliance of the PPSD Decentralized Security Program and Guidelines and the IPA.
- If the Authorizing Official/Manager separates at any time during the year, a newly appointed Authorizing Official/Manager must complete and resubmit the PSD041.

NOTE: Failure to provide the Annual Statement of Self Certification by January 31 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 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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Technology Services (OTECH) – Service Desk</td>
<td>(916) 464-4311</td>
</tr>
</tbody>
</table>

SCO ISO Help Desk Hours: 8:00 am - 5:00 pm (916) 322-8094