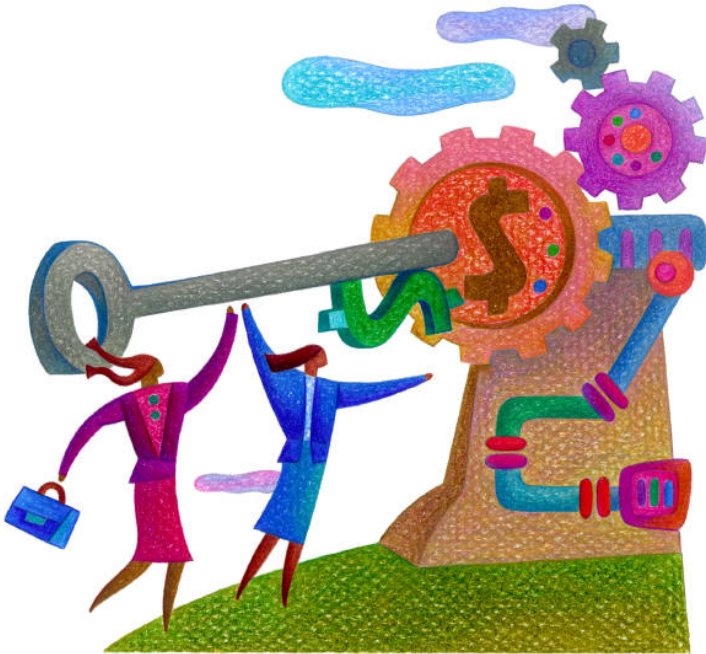


PPS BASICS: ACCOUNTABILITY



ACCOUNTABILITY

- Accountability is the delegation of authority and responsibility to qualified persons to initiate, process, and review business transactions and holding those persons responsible for the validity, correctness and appropriateness of their actions.

So what does that
really mean to you?



Is PPS Data Confidential?



- Isn't all that PPS information public information?
- Is somebody's salary, age, race, home address protected information?

Is PPS Data Confidential?



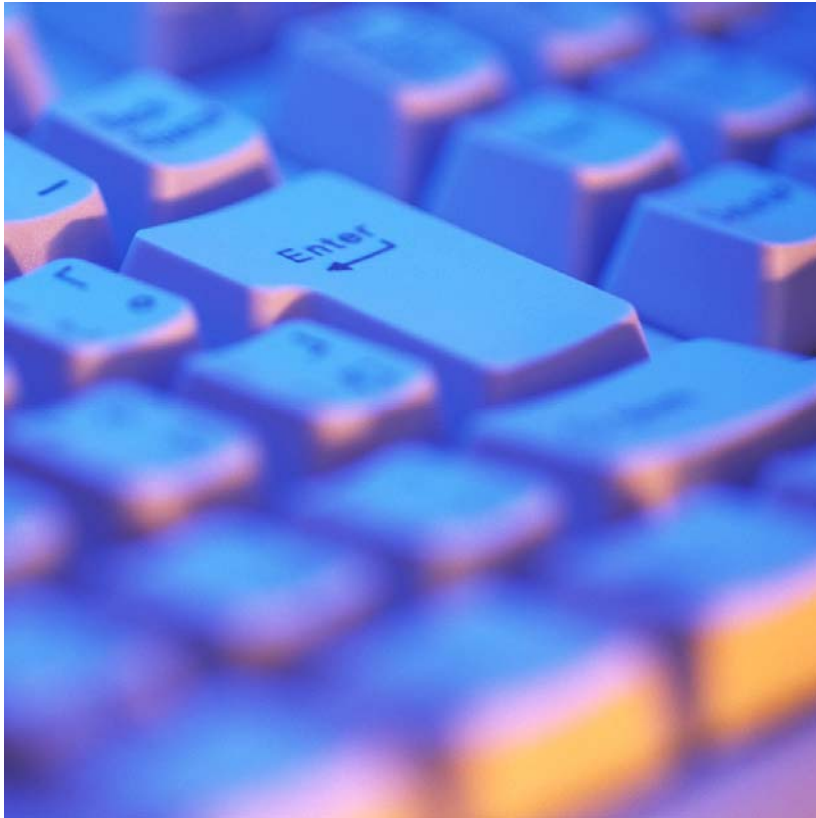
- Can you share an employee's salary info with a co-worker?
- Can a manager ask you to share the salary of another manager?
- Can you use PPS to find the home address of an employee for your holiday card list?
- Can you use PPS to find out how old all the Professors are in your department?

What's your role?

- Do you just process whatever you get?
- Should you ask questions?
- Should you make sure you have appropriate documentation?



You are Accountable



You have the responsibility and authority to conduct University business through the Personnel Payroll System.

You are not the only person accountable in the process, but you are responsible for your individual actions.

BUILD YOUR CONFIDENTIALITY MUSCLE!



REQUEST FOR ACCESS TO PAYROLL PERSONNEL SYSTEM (PPS)

RETURN FORM TO: Accounting Services & Controls, Mail Code 2040, or Fax to: Computing Support (x8682)
 For further explanation of PPS roles and responsibilities, please see the "Advice to Managers" at <http://hr.ucsb.edu/hris/pdf/advice-to-managers.pdf>

Please use this form to request access for the user responsible for: PPS Inquiry, Entry/Update, Time Reporting, PAN distribution and/or Web Merit Functions. Please allow two business days for processing, and please see the third page for terminology explanations.

Accounting to Assign	<input type="checkbox"/> Add (new account): Transferring to a new department or a new employee to the university.	<input type="checkbox"/> Modify: Making changes to an existing account.	<input type="checkbox"/> Delete: Transferring to a new department or separating from the university.
New Logon ID: <u>SB</u>			

If applicable, existing ID: SB Date Last Used PPS: _____ Employee ID: _____

User's Name: _____ (please print name: LAST, FIRST, MIDDLE) Job Title: _____

Department: _____ *Phone: (805) _____ *E-mail: _____

Please fill out the fields this user will be responsible for.

<p>**Designated Manager <input type="checkbox"/></p> <p>**DSA <input type="checkbox"/></p> <p>Computer Support Coordinator <input type="checkbox"/></p> <p>If you have any of the above responsibilities, please check if you require a PPS account:</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p>	<p style="text-align: center;">INQUIRY</p> <p>Functions: Inquiry <input checked="" type="checkbox"/></p> <p>Access Rules:</p> <p>Universal Access (Central Office Functions Only) <input type="checkbox"/></p> <p>Control Point <input type="checkbox"/></p> <p>Individual Depts. <input type="checkbox"/></p> <p>Please list 4-letter dept. codes: _____</p> <p>Additional Restrictions:</p> <p><u>Appointment Type</u></p> <p>None <input type="checkbox"/></p> <p><u>Personnel Program</u></p> <p>None <input type="checkbox"/></p> <p><u>Student Status</u></p> <p>None <input type="checkbox"/></p>	<p style="text-align: center;">PREPARER</p> <p>Primary <input type="checkbox"/></p> <p>Back-up <input type="checkbox"/></p> <p>Functions to be prepared:</p> <p>Entry/Update <input type="checkbox"/></p> <p>Time Reporting <input type="checkbox"/></p> <p>Access Rules:</p> <p>Universal Access (Central Office Functions Only) <input type="checkbox"/></p> <p>Control Point <input type="checkbox"/></p> <p>Individual Depts. <input type="checkbox"/></p> <p>Please list 4-letter dept. codes: _____</p> <p>Additional Restrictions:</p> <p><u>Appointment Type</u></p> <p>None <input type="checkbox"/></p> <p><u>Personnel Program</u></p> <p>None <input type="checkbox"/></p> <p><u>Student Status</u></p> <p>None <input type="checkbox"/></p>	<p style="text-align: center;">PAN REVIEWER</p> <p>Mandatory <input type="checkbox"/></p> <p>Back-up <input type="checkbox"/></p> <p>Functions to be reviewed:</p> <p>Entry/Update <input type="checkbox"/></p> <p>Time Reporting <input type="checkbox"/></p> <p>PAN Routing Rules:</p> <p>Universal Access (Central Office Functions Only) <input type="checkbox"/></p> <p>Control Point <input type="checkbox"/></p> <p>Individual Depts. <input type="checkbox"/></p> <p>Please list 4-letter dept. codes: _____</p> <p>Other Routing Rules: _____</p>
<p style="text-align: center;">MERIT ACCESS</p> <p>Control Point <input type="checkbox"/></p> <p>Department(s) <input type="checkbox"/></p> <p>Please list 4-letter dept codes: _____</p>			

Access to the PPS is granted based on your need to know the information for performance of your assigned job duties. Misuse or abuse of computer resources is a serious matter that may constitute violations of federal and/or state criminal statutes for which prosecution will be pursued in accordance with the California Information Practices Act, and the Privacy Act of 1984. Employees with access to personal and confidential records shall take all necessary precautions to assure that proper safeguards are established and followed to protect the confidentiality of records. Employees may not disclose personal or confidential information concerning individuals to unauthorized persons or entities as specified by Personnel Policy and Collective Bargaining Agreement. Violation of relevant policies and legislation could result in penalties such as suspension, termination, expulsion or fines.

Signature of Person Receiving Access _____ Date _____

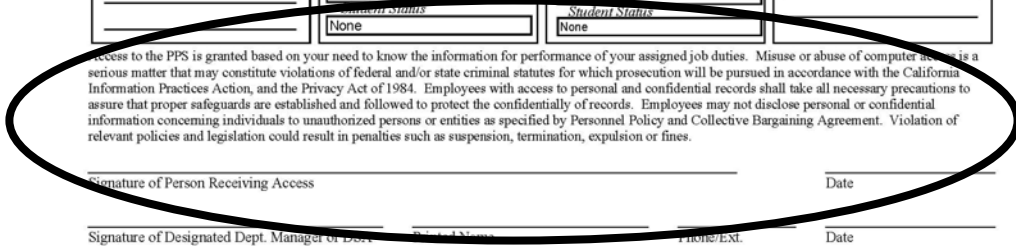
Signature of Designated Dept. Manager or DSA _____ Phone/Ext. _____ Date _____

If this request is a change in the Designated Manager and/or DSA access, Department Chair/Director must sign below:

**Signature of Dept. Chair/Director _____ Printed Name _____ Phone/Ext. _____ Date _____

Accounting Office Use

Accounting Check by: _____ Date: _____ User ID: _____ Screen Group: _____



READING THE FINE PRINT

- Access to the PPS is granted based on your need to know the information for performance of your assigned job duties. Misuse or abuse of computer access is a serious matter that may constitute violations of federal and/or state criminal statutes for which prosecution will be pursued in accordance with the California Information Practices Action, and the Privacy Act of 1984. Employees with access to personal and confidential records shall take all necessary precautions to assure that proper safeguards are established and followed to protect the confidentiality of records. Employees may not disclose personal or confidential information concerning individuals to unauthorized persons or entities as specified by Personnel Policy and Collective Bargaining Agreement. **Violation of relevant policies and legislation could result in penalties such as suspension, termination, expulsion or fines.**

Standards of Ethical Conduct

- We hold the University in trust for the people of the State of California.
- We are expected to conduct ourselves ethically, honestly and with integrity in all dealings.
- We are expected to transact all University business in conformance with policies and procedures.
- It is not acceptable to ignore or disobey policies if one is not in agreement with them, or to avoid compliance by deliberately seeking loopholes.

Who decides? Who approves?



- Can you process your own salary increase?
- Can your manager direct you to increase his/her salary?

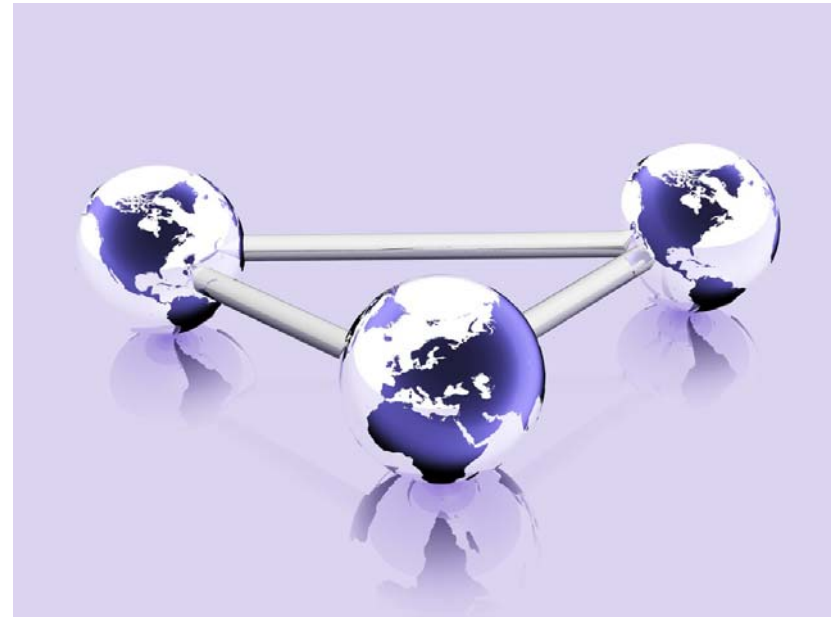
Everyone is Accountable

- Employees should use University computing resources only for legitimate University business purposes that the employees have been authorized to perform. Updates to PPS must meet applicable policy and procedure requirements.
- Updates to the PPS must meet applicable policy and procedure requirements.
- Privacy and confidentiality of information contained in the system must be maintained.



Separation of Duties

- Separation of duties is the universally recognized internal control principle that more than one qualified person should be involved in initiating, recording, and reviewing every financial transaction or business action with financial aspects in order to reduce the risk of error or inappropriate actions.



Control Features of PPS

- Will not allow an employee to update his/her own record.
- Requires at least one mandatory reviewer.
- Departments are required to assign separate individual the roles of preparer, reviewer, and backup preparer/reviewer.

What would you do?

- What if you are asked to do something you think is unethical, violates UC policy and/or may be illegal?



CALL A FRIEND

- There are many resource people on campus who can help you do things the right way.



Campus Resources

- Human Resources
 - Coni Edick
- Accounting Services & Controls
 - Sandra Featherson
- Academic Personnel
 - Cindy Ponce
- Audit & Advisory Services
- Whistleblower Coordinator
- Office of the Ombuds

ROLES IN PPS



ROLES IN PPS

Designated Manager

Primary Preparer

Mandatory Reviewer

Backup Preparer/Reviewer

Department Security Administrator (DSA)

Department Head or Designated Manager

- Reviews the accountability structure to ensure that it follows accepted accountability principles including separation of duties
- Monitors delegations and procedures to ensure they remain secure, accurate and current
- Insures all departmental personnel have participated in the required training and are performing their duties according to policies

Preparer

- Understands the transaction and ensures that prior authorization is obtained
- Understands policy and regulatory requirements
- Ensures that appropriate and accurate data are entered
- Resolves questions raised during entry via on-line edits and error messages
- Notifies the DSA and/or Department Manager of absences so that backup can be implemented
- Accepts responsibility for all entered PPS transactions

Mandatory Reviewer

- You are the safety net!



Mandatory Reviewer

- Reviews transactions within two business days
- Reviews each transaction for compliance with policy
- Ensures that questions are resolved within two business days or that the transaction is reversed until it is resolved
- Notifies DSA or Department Manager of any absence of more than two days
- Accepts accountability for reviewing PPS transactions

Backup Preparer/Reviewer

- Receives training equivalent to primary preparer and/or mandatory reviewer
- Fulfills same responsibilities as primary preparer or mandatory reviewer
- Maintains currency of knowledge

Data Security Administrator (DSA)

- Records all accountability delegations
- Contacts accounting to provide appropriate access for all on-line preparers and the designated PAN reviewers of a department's on-line transactions
- Updates the record of accountability delegations each time a change is required such as when a person is absent and back-up is assigned, or when an individual leaves, is hired, or responsibilities change.

PASSWORD MANAGEMENT



PASSWORDS

Your password authenticates your identity to the system. Do **NOT** share your password with **anyone**. Allowing another person to use our password violates the principles of system user accountability.

Specific PPS Password Requirements

- The minimum length of PPS passwords is 7.
- Your password must contain at least 1 digit and 1 alpha character in the password you create. On PPS, password is not case sensitive.
- Change your password at least every 6 months, or whenever you suspect its confidentiality may have been compromised.

Basics of Password Management



- Select a password that does not form an English language word.
- Select a password that you can easily memorize, but hard for another person to guess.

Password Management

NO!

FLUFFY1

JILOGON

PPSLOGN

Yes!

TQBFJOTLD

Duk!w2SJ?

M\$8ni3y0



Log off Log Out



- Employees should log off the system whenever they leave their work stations unattended in order to protect the system from unauthorized access and use

A log on ID is considered equivalent to a signature and an employee is responsible for all entries made under his/her log on ID.

THANKS!

