1.3 SYSTEM ACCESS

PPS User Access

Access to the Payroll/Personnel System (PPS) is granted to employees whose official job duties require access to PPS data for business purposes. It is the responsibility of the approving authority (i.e., the Data Access Grantor) to ensure that granting access to an employee is appropriate. Access is restricted to inquiring, updating and/or reviewing employee records within the user's purview. Typically these are categorized as the unit; the service center, which includes records for all units/boards served; the principal officer jurisdictional area, which includes all units reporting to the principal officer; and the central office, which generally includes access to all employee records. Access to the PPS is provided only after the appropriate training program has been successfully completed (e.g., an individual approved for Inquiry access must take PPS Basics Training prior to gaining access to the PPS). Types of access, PPS data information types, criteria for granting access, data access authorization (Data Access Grantor), and revoking access are discussed below.

Ensuring Appropriate Access

Types of PPS Access

The Data Access Grantor is accountable for ensuring the person is requesting the correct type of PPS access to complete their job duties. There are two types of access granted to the PPS. The type of access depends on the job responsibilities of the employee. Any current PPS User whose type of access changes (e.g., from "Inquiry" to "On-line Entry Update") is required to have their account updated using the ITS Computer Account Modification Form. The types of access are:

Inquiry

Inquiry (includes History & PAN) allows users to review payroll/personnel information for employee records within the user's purview (i.e., unit, service center, principal officer's jurisdictional area, or central office). Inquiry access is provided to individuals whose job responsibilities require them to utilize payroll/personnel information. This is also the level of access needed for an individual assigned Post Authorization Notification (PAN) Reviewer duties. This access does not provide the ability to enter transactions via On-Line Entry Update (OEU).

On-Line Entry Update (OEU)

On-Line Entry Update access allows users (i.e., preparers) to input or modify data to which they have access rights. OEU access is restricted to central office and service center staff. Preparers automatically have inquiry access to review payroll/personnel information and historical records within their purview.

Educating to Protect Privacy Rights

The Data Access Grantor is accountable for educating each person granted PPS access about their responsibility in protecting the privacy rights of every employee by not disclosing data pertaining to an individual's personal information.

Per University policy Business and Finance Bulletin RMP-8 there are three classifications of information for disclosure purposes and different rules apply for each type. The classification and rules are based upon the Public Information Act and the Information Practices Act which define public information and also address individuals' privacy rights. Any employee who divulges non-disclose personal information could be subject to disciplinary action by the University as well as civil suit by the person(s)

whose personal information was disclosed. All information contained in the PPS database falls into one of the two classifications listed below. (See the *Business and Finance Bulletin RMP-8* for more detailed information: *http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html.)*

Public Information

This is information which is not identifiable to an individual and, generally, it may be made available upon public request. However, there is some information identifiable to an individual which is defined as Public Information in the California Public Records Act and can be disclosed. This includes name, date of hire or separation, current position title, current rate of pay, organization unit assignment including office address and telephone number, current job description, full-time or part-time, career or casual, or probationary status, prior non-University employment and other information as determined by University General Counsel.

Non-Disclose Information

This includes personal information that can be identified to an individual. In most cases, personally identifiable information is protected from disclosure under privacy laws. Examples of personal information that is protected from disclosure include sex, ethnicity, birth date, and social security number. The University will not disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the disclosure of the information meets one of the requirements in *Business and Finance Bulletin RMP-8 Section VII.G.4*.

Access Authorization

Data Access Grantor

The Data Access Grantor (DAG) is the individual who approves the appropriate type of access (i.e., Inquiry or On-line Entry Update) based on business purpose (job duties and/or need-to-know basis) by signing the UCSC Academic/Administrative Account Form. Generally the Data Access Grantor is the unit manager or respective principal officer. PPS Data Access Grantors have been delegated authority by their Senior Officer. This authority cannot be redelegated except by the Senior Officer. The list of current authorized PPS Data Access Grantors (including alternates) is available upon request from the PPS Office.

Criteria for Granting Access

Job Duties and Need to Know

Before the UCSC Academic/Administrative Account Form for PPS access is completed, the DAG needs to review the roles and responsibilities assigned to each person who is involved in payroll/personnel activities. The Data Access Grantor is accountable for ensuring there is a business justification for requesting PPS access for the employee and that adequate separation of duties exists.

All persons must have a business justification to inquire, prepare or review PPS data before access is granted. Generally, this justification is reflected in the individual's job description. There are some instances in which a person is granted inquiry access based on their "need to know," which isn't always as clear-cut as the performance of preparer and/or mandatory reviewer job duties. Because of the need to protect employees' privacy rights, access should be denied whenever the person's need for PPS data is limited or other sources exist to provide the information.

Data Access Examples

The following examples are representative of different situations and issues that may arise as Data Access Grantors decide whether authorizing PPS access to an employee is justified. The examples are not intended to be inclusive of all situations.

- Person A serves as the Preparer of PPS transactions affecting employees in units served by the service center. Person A is assigned duties that *require* On-Line Entry update (OEU) Access to PPS in order to perform their job duties.
- Person B serves as a Mandatory Reviewer of PANs, however, Person B does not perform OEU duties. Granting access to "Inquiry" is justified based on the job duties. There would be no business justification to provide "OEU" access.
- Person C serves as an administrative assistant in a large unit whose payroll/personnel transactions are prepared by its service center. Person C is often the contact person with the service center on behalf of the unit head and, for example, communicates with the service center about student and casual staff employee extensions of time. At times, it is necessary for Person C to access personnel information to facilitate this communication. There is a need-to-know justification for granting "Inquiry" access to Person C; this access would be restricted to employee records associated with the unit.
- Person D is a unit head. While Person D can always request personnel information from the Service Center, it is useful to Person D to have information about classification, salary, and duration of temporary appointments available for planning purposes. There is a need-to-know justification for granting "Inquiry" access to Person D; this access would be restricted to employee records associated with the unit.
- Person E is a temporary employee hired for three months until a replacement can be hired for a payroll assistant who terminated. Because the individual must successfully complete the appropriate training prior to gaining access to the PPS, the manager will need to determine the viability of granting access. The manager may want to consider other options: Can the PPS data that Person E requires to perform their job duties be provided from another source or via an employee who has authorized access? Can the job duties requiring PPS access be temporarily reassigned to another employee with appropriate PPS access? A factor may be the length of time of the position. That is, the longer the duration of the position, the more viable it may be to invest in Person E's training and grant access.
- Person F enters PPS data for staff employees and is the mandatory reviewer for academic employee data *entered by Person G*. Person G is the mandatory reviewer for the staff data *entered by Person F*. Both Person F and Person G have a business need-to-know reason to be granted OEU access which is restricted to employee records associated with the unit.
- Person H works in a Central Unit (such as human resources, payroll, benefits, student employment). Person H looks up PPS data on-line in response to inquiries from campus employees. There is a need-to-know for Person H to be granted universal “inquiry” access to the PPS.
- Person I is a computer coordinator with responsibility for ensuring that network communication software, PCs and printers are properly set-up to allow the user entry into PPS. Person I does not have a business need-to-know reason to be granted access to PPS. The ITS Help Desk and central offices are responsible for assisting users with questions about PPS.

Further information concerning access to records is found in *Business and Financial Bulletin RMP-8*.

Certification

To request an application for access to the PPS (UCSC Acacemic/Administrative Account Form, pp. 1 and 2) and an Access to Information Statement, contact: ITS Help Desk at: 459-HELP (4357).

Your application must be approved by the appropriate PPS Data Access Grantor for your service center or unit, and be submitted to ITS for processing, along with the Access to Information Statement with your signature.

If you have not already contacted the PPS Office to enroll in the next available training, the PPS Office will contact you to enroll in the appropriate training:

- **PPS Basics Training**
  (for Inquiry-only users and Non-Mandatory PAN reviewers)

  Successful completion of PPS Basics Training requires the demonstration of specific inquiry skills.

- **PPS Training Program for Preparers, Mandatory Reviewers and their back ups.**

  This training is available to those employees who have been assigned PPS preparer or reviewer duties and been approved by the appropriate PPS Data Access Grantor. Attendance at all appropriate modules is required.

  Successful completion of the PPS Training Program includes demonstration of specific skills covered during training and endorsement of all trainers.

Upon successful completion of the appropriate training, participants will receive a Certificate of Completion and ITS will be notified to complete the access process. The ITS Help Desk will contact the user when the account has been set up and is ready to access.

Records of PPS training completion, modules taken, and certification are maintained by the PPS Office.

Revoking Access

There will be situations where termination of PPS access is required or deemed necessary. Voluntary or involuntary termination of employment will require termination of PPS access for the individual. There may be other situations where it is appropriate to revoke access to the system, such as, change in job duties, transfer to another campus unit, violation of confidentiality, accessing data not based on an employee's "need-to-know," or sharing of passwords. Managers are accountable for immediately notifying the ITS Help Desk at x4357 to delete all system access for the employee. The Help Desk will need the employee's name and PPS User ID.

Temporarily Locking PPS Access

If an employee goes on a temporary leave from their PPS position (e.g., vacation, furlough, temporary leave to work in another campus unit) the Service Center Manager is responsible for notifying ITS to have the employee's PPS Access "locked."

Procedures for Locking PPS Access

1. The Service Center Manger must send written authorization (e.g., email) to the PPS Office (pps_office@ucsc.edu) that this employee will be on leave for a given period of time and the account should be locked for the duration of the leave. The employee's supervisor can also submit such a request.

   Note: If this is a Mandatory Reviewer, the Service Center Manager must also notify the PPS Office, that the PAN Routings should be routed to the Back-Up Mandatory Reviewer during this period of time.

2. The PPS Office will lock the PPS Account per this notification from the Service Center Manager or Supervisor and the PPS Office will make the appropriate adjustments to the PAN Routings, if necessary.

3. Upon return, the employee will need to contact pps_office@ucsc.edu to request a new password.

4. If this was a Mandatory Reviewer, the Service Center Manager or Supervisor will need to complete the loop by notifying the PPS Office that the PAN routings should be returned to their original set-up.

System Passwords

Password Selection and Security

Passwords should be eight alphanumeric characters and may also include the following special characters: @, #, and $. You are required to create a password that is a combination of alphabetic and numeric characters; try to choose a password that is easy to remember, yet difficult for someone to guess. For more information on UCSC password strength and security standards, see http://its.ucsc.edu/security/policies/password.php

Maintaining the confidentiality of passwords is an essential safeguard against misuse, intrusion, and theft. **You are personally responsible for the use of your User ID and password.** If there is a reason to suspect that password confidentiality has been compromised, you are responsible for changing the password immediately and reporting the suspicion to the ITS Help Desk.

Password Expiration

All passwords automatically expire every 6 months. When a password expires, you are prompted to enter a new password. All passwords must be unique for 13 months and cannot be reused during that period.

Invalid Logon Attempts

If you attempt to log on with a valid User ID and an incorrect password, the message Password Invalid is displayed. After 5 invalid password attempts, the User ID is automatically revoked and you will need to contact the ITS Help Desk to reactivate your User ID.

Security

When leaving your computer, for a short period of time (10-15 minutes) after you have logged onto the system, enter **!L** and press **Enter** in the Next Function field to lock the keyboard and screen (see *Section 1.5, Navigation and Entry/Update Commands*, for more information). When you leave your computer for longer periods, always log off completely. Logging off frees system resources for other users and closes the connection to the UCOP computer.