PeopleSoft Security Glossary

Overview of PeopleSoft Security

What is PeopleSoft Security?

UserID / User Profile → Role, Role, Role ← Permission Lists / Access to pages & actions

Row Level Security / Primary Permission List, Emplid

Roles - collection of permission lists

Permission lists controls access to particular or combination of page(s)/screen(s), sign on time, etc.

Row level security controls data access by the institution/college, business unit, department etc.

Understanding PeopleSoft Security

Understanding PeopleSoft Security

PeopleSoft security is based on permission lists and roles.

Image: A user's security profile is made up of permission lists and roles

This diagram illustrates how permission lists are assigned to roles and then roles assigned to user IDs to create user security profiles:

To administer security:

1. Create permission lists.
2. Create roles and attach permission lists to roles.
3. Create user IDs and attach permission lists and roles to user IDs.

Administering User Profiles

User security profiles are made up of the combined permissions of the roles and permission lists assigned to them

PeopleSoft Security Hierarchy

To get your mind around PeopleSoft security, it helps to look at the hierarchy for PeopleSoft security. From top-to-bottom (highest to lowest level of granularity) you can look at security like this:

- Portal Security
  - Menu Security
    - Roles
      - Permission Lists and Definition Security
        - Primary Permission Lists
          - Row Level Security (user & permission list based)

- Portal folders (containers in the left navigation) are secured by permission lists at the portal level
- Portal content references (links on the left navigation) are based on menu security
- Roles give users access to one or more permission lists
- Permission lists give users access to menus, components and ultimately pages
- Definition security is used by application designer to secure definitions (e.g. fields, records, pages, components)
- Primary permission lists typically control row level security. For example, in HCM, primary permission lists are used to control access to departments.
- Row level security gives specific users access to specific data. For example, in Campus Solutions, specific users can be given access to a particular academic institution. This can also be permission list based.

Academic Structure Chart (Campus Solutions - Row Level Security)
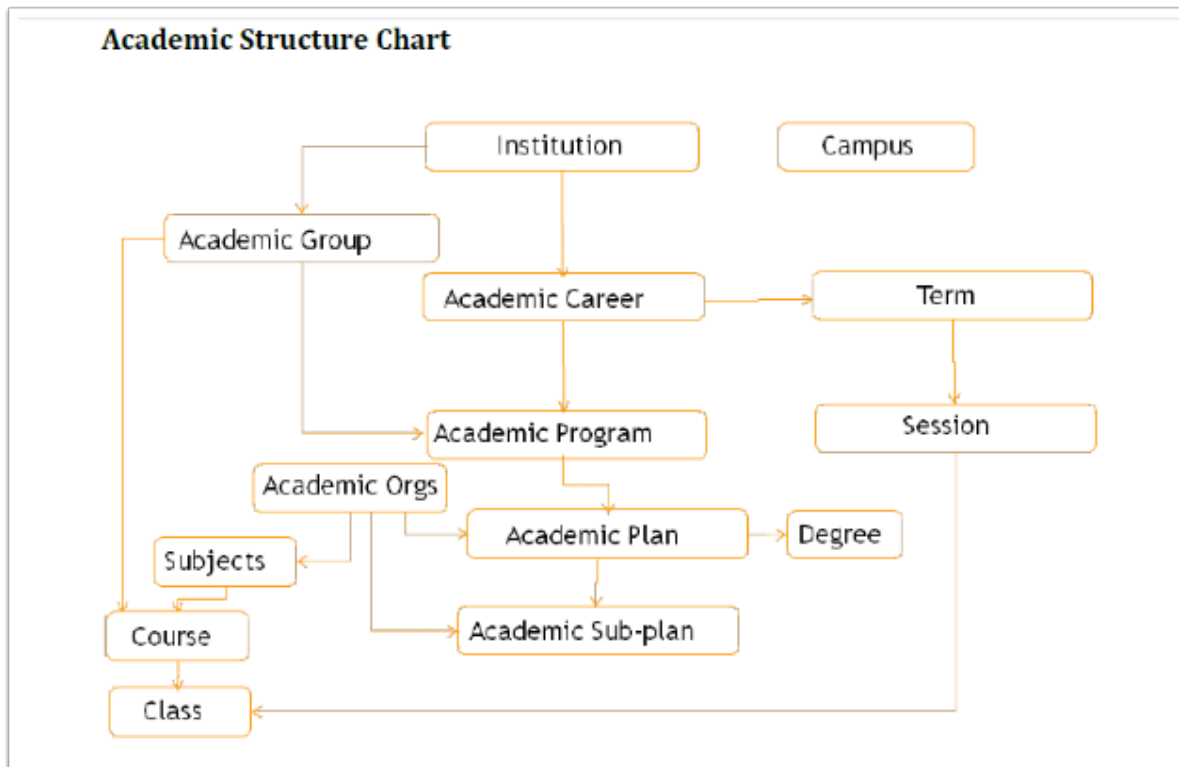

Academic Structure Terminology Defined

- **Academic Institution** is an independent entity that has its own set of rules and business processes. Institutions: Tacoma and Spokane District, Spokane Falls Community College, and Spokane Community College
- **Academic Campus** is where your campus is located
- **Academic Organization** Department and Schools
- **Academic Career** includes the following two categories: CNED (Continuing Education) and UGRD (Undergraduate)
- **Academic Programs** students are admitted and matriculated in Academic Programs. This identifier drives key business processes such as academic standing, grading, billing and financial aid.
- **Academic Plan** is an area of study within a career or program.

Academic Structure is the foundation of the Student Information System Campus Solutions and defines your college within the PeopleSoft system. The chart above shows how the components of the Academic Structure relate to one another. Academic Structure can be understood as two interrelated parts: a student's program of study and courses, classes, and the departments that own them.

SACR Row Level Security in PeopleSoft (screen shot)
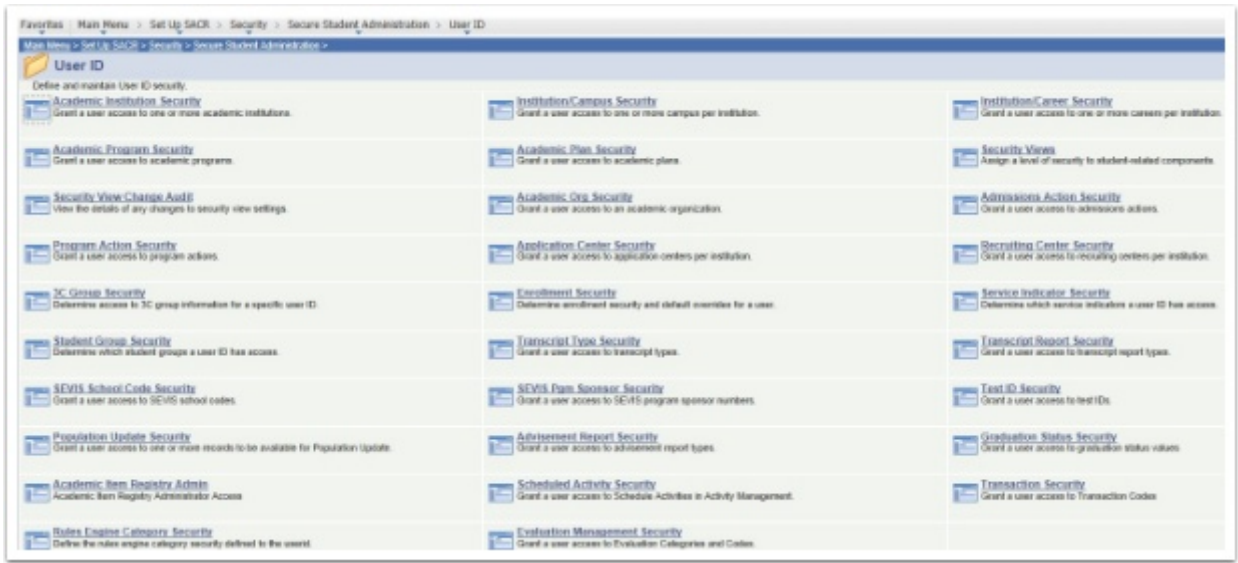
HCM Transaction Security Data

This diagran shows the Department field being used as transaction security data to secure the data of people in the organization in which the user only has security access to the workers in department 123:

The department field is the transaction value securing the data rows
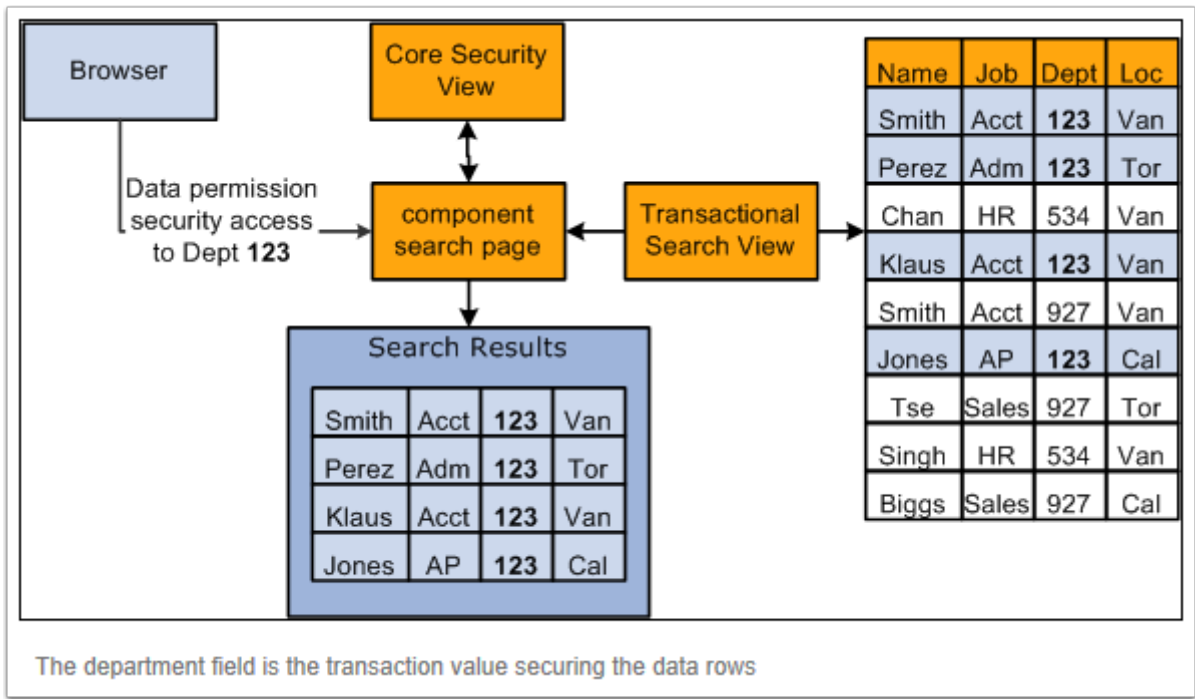
User security data is the data about a user's security access. It enables the system to ensure that users have access only to that which you have granted them access. User security data for

---

HRMS data permission is the data permission that you assign to permission lists and the roles and users to whom you assign the permission lists.

Data permission is granted to row-security (tree-based) permission lists (ROWSECCLASS) and regular (role-based) permission lists (CLASSID). When you create a permission list on the Permission Lists component you can assign security to a number of different aspects of the application. Data permission is assigned separately on the Security by Dept Tree page and Security by Permission List page.

HCM ROWSECCLASS Data Security Model

This diagram shows that permission lists are created, assigned data permission (using either security by department tree or security by permission list), and then assigned to a user directly on the User Profile-General page as the Row Security permission lisst or assigned to a user on the User Profile - Roles page by assigning roles to the user, which are associated with permission lists:

Create permission lists, assign to them data permission, and assign them to users
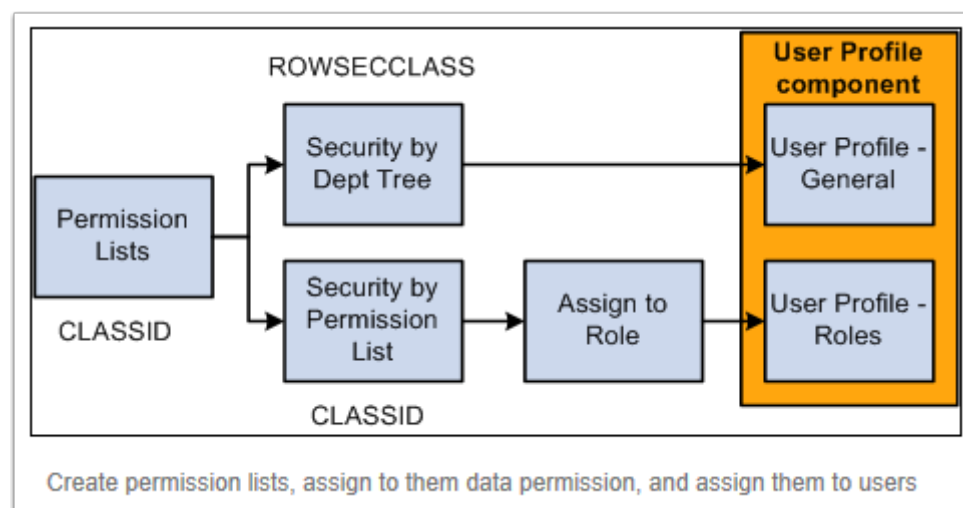
HCM Search Page Results based on Row Level Security assigned by Primary Permission List

This diagram shows the search page determining which permission lists a user has and what data permission the list gives the user. The user, TRN, is associated with the permission list TRAIN for both row security and permission lists through roles. Since permission list TRAIN is granted access to worker's records in department 123 only, the search results will display only those workers from this department. The system determines which permission lists a user has and what data permission is granted by the permission list before retrieving the matching data rows.
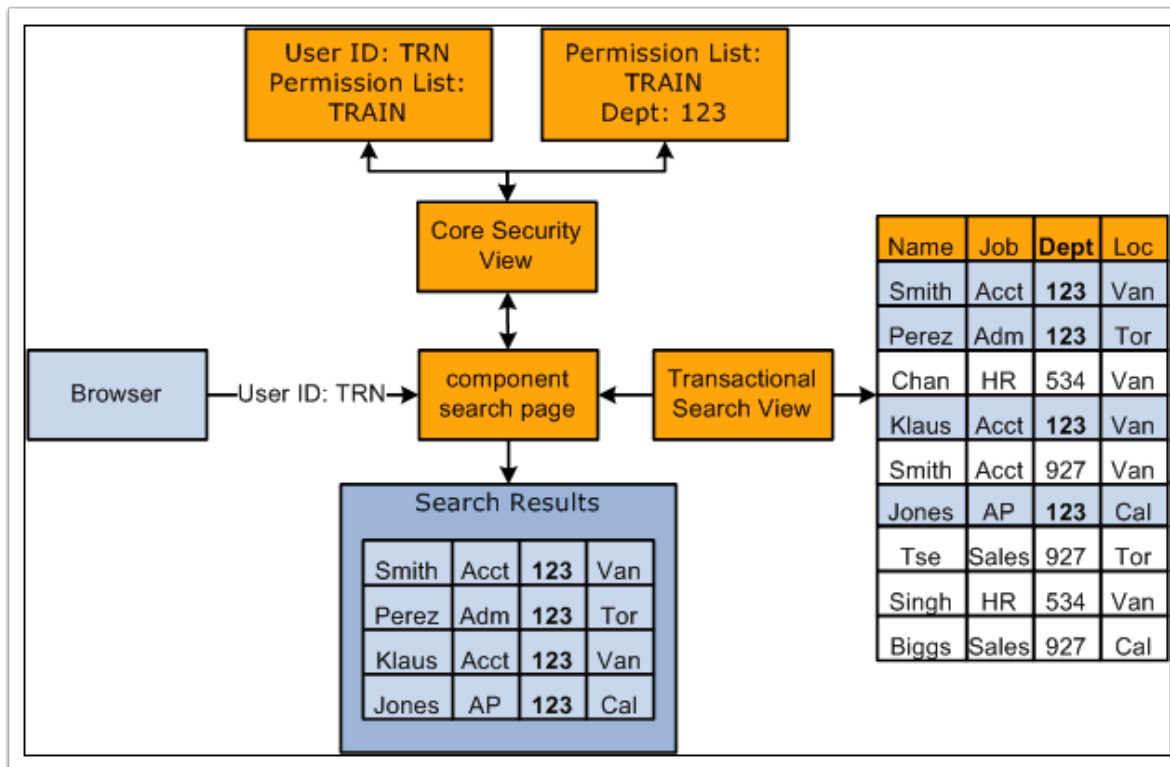
Shift+Ctrl+J key

Navigation: Main Menu > Records and Enrollment > Career and Program Information > Student Program/Plan

1. When on this PeopleSoft page or any other page in PeopleSoft, press the **Shift+Crtl+J** key simultaneously.

2. Results below:

Browser	OTHER/O
Operating System	WIN7
Browser Compression	ON (gzip)
Tools Release	8.53.10
Application Release	HRMS and Campus Solutions 9.00.00.000
Service Pack	0
Page	**STDNT_PROG**
Component	**ACAD_PLAN**
Menu	**TRACK_STUDENT_CAREERS**
User ID	CTC_XXXXXXX
Database Name	CSDV6
Database Type	ORACLE
Application Server	//s616183se2vl168:9040
Component Buffer Size (KB)	585

This page identifies the Page, Component, and Menu:

Page: STDNT_PROG

Component: ACAD_PLAN

Menu: TRACK_STUDENT_CAREERS

Glossary of Terms

PeopleSoft applications use multi-level security to enable you to successfully manage shared data environments. You set up data access at different points within your system and define the most efficient path to data across business groups, tables, departments, and pages. You have full control over security definitions, selecting options to create a matrix that enables or restricts user access to data through a series of authorizations.

Menu, Components & Pages		It is important to understand the basic concept of how PeopleSoft pages are developed in terms of Menu & Compone structures.
Components	Components are PeopleSoft pages and groups of pages. These are the screens or pages that you access in PeopleSoft to perform various actions and/ or view.	The student center is a collection of PeopleSoft components. **Security Troubleshooting** To see the name of the PeopleSoft page and component you a accessing, press **Shift+CTRL** (Control Key) and the **"J" Keys** *simultaneously*. **Shift+Ctrl+J.** **Shift+Ctrl+J provides pertinent security information for yo Security Administrator.** **See example at the end of this document.**
Page	A page is assigned to a Component group that may contain multiple pages and the actions available for any particular Page.	**Actions:** Add (A), Update/Display (UD), Update/Display All (UDL), and Correction (C). There is also a Display (D) only action – giving access to

		view only.
Menu	Each component is assigned to a Menu Group.	This is the PeopleSoft Navigation you access in the application.
Navigation	The path by which you can get to any given page in PeopleSoft. It is generically referred to as the "navigation".	The navigation appears at the top of your menus in the blue area. For example: Main Menu Student Financials Refunds
Permission Lists, Roles and User Profiles		Just as it is important to understanding how Menus, Pages, and Components are developed, it is also important to understand how they are secured.
Permission lists	Permission Lists – controls access to particular or combination of page(s)/screen(s), access time, query and process security. Building block or "heart" of PeopleSoft Security. All page access is defined on a Permission List Level. This is where page access is granted as well as other security options. Permission lists are then assigned to Roles, which are then assigned to Users. You cannot give page access to a user directly.	Permission List contains pages and their access options. For example, there is a page called, "MyPage". You add the page to a Permission List with specifications for its access (Add, Update/ Display, Update/Display All, or Correction)
Role	A collection of permission lists. Permission list(s) is assigned to a Role. The Role is simply a structure that "holds" one or more Permission Lists. Roles are the intermediary step between Permission Lists and User Profiles. They allow groups of Permission Lists, usually based on a user's job role, which are then assigned to User	Let's say we assigned the "MyPage" page to a Permission List called MyPermissionList. You would then assign MyPermissionList to the MyRole. Note: A Role can contain multiple Permission lists.

	Profiles.	
User Profile	A definition that represents an application user.	Assign role(s) to a User Profile. MyPage is assigned to MyPermissionList. MyPermissionList is assigned to MyRole. MyRole is assigned to my User Profile. User now has access to MyPage.

	The User Profile is the actual "account" for a user in PeopleSoft.	See Diagram 1.1 – Diagram 3.1 and Appendix A at the end of this document for visuals on PS security: user ID, roles, and permission lists.
Emplid	Pronounced EMPULL-ID, it is the student and/or employee number assigned to every person in the PS system. Emplid is the number that PeopleSoft uses to identify an individual person in the system. Every person in the Campus Solutions system will have a unique Emplid assigned to them. At ctcLink , your 9 digit number will serve as your Emplid.	It is not the student's or employee's social security number. Emplid is assigned to the user profile.
User	Controls access to application pages, functions, and business components.	
Overview of Row Level Security	Controls data access by the institution/college, business unit, department, etc. an application user belongs to. This term could be used differently in	PeopleSoft determines Row Level Security by using settings associated with both the Primary and Row Security Permission Lists. These Permission Lists are used to control the actual data within a table that can be accessed by a particular user based on an attribute such as Department,
	different applications, for example, Campus Solutions: row level or SACR (Student Administration Contributor Relations) security. HCM: core row level security (transaction data security) Financials: row level security Row level access can be controlled by user or by Primary Permission list for groups of users needing the same access.	Business Unit, or SetID. CS row level security is assigned to individual users but can be assigned using a tool. HCM and FS use a primary permission list to control row level security.

Row Level Security	Controls access to the subset of data rows within tables that the user is authorized to review or update.	Individuals are assigned row level security based on their job functions.
Field Level	Controls access to individual fields on pages.	
National ID DOB masking	Social Security Number and Date of Birth (DOB) are masked in your searches. Last 4 digits of the SSN and year in birthdate. You can do most person look-ups by national ID when it is provided to you.	999-99-5231 masked: XXX-XX-5231 07/11/1954 masked: 07/11 In Campus Solutions SSN DOB masking are controlled via a Primary Permission List that is attached to user profiles. Three primary permission lists control masking: MASK ALL – Mask fields of National ID and Birth Date MASK PARTIAL – Mask partial fields of National ID and Birth Date MASK NONE – No masking of fields National ID and Birth dateDefault masking for most users is MASK PARTIAL

Campus Solutions SACR Row level security		
Institution Structure	Institution, Academic Career, Programs, Plans and Degrees.	Assign a specific Institution to a user as well as other Academic data such as Career, Programs, and Plans. This provides access to the data that users need to do their jobs. See Diagrams 4.1 Academic Structure Chart for an understanding of Academic Structure and securing Institution, Academic Career, Academic Program, and Academic Plan row level security.
Academic Institution Security	Grants users access to Institutional data	Assign value(s) based on user's Institution and access WA171 – Spokane CC WA172 – Spokane Falls WA220 – Tacoma CC Can assign multiple values to one user

Institution/ Campus Security	Grants users access to Campus	Campus value is "Main" regardless of the Institution If a user is in multiple Institutions assign Campus security for each Institution.
Institution/ Career Security	Grants users access to Careers	Values: CNED (Continuing Education) and UGRD (Undergraduate) User may only be assigned responsibility for the CNED career.
Academic Program Security	Grants "all" or specific programs to a user. User cannot change a student's program without security to that program.	Can assign "All" programs to a user or limit programs by only assigning security to the programs that the user needs to access.

		User may only have access to accounting programs for the accounting department. Must be done for each Institution.
Academic Plan Security	Grants Plan security to users	Can assign "All" plans to a user or specific plans. For instance, user may only have responsibility for accounting plans. User cannot assign or remove a plan from a user without security to that plan.
Academic Org Security	Grants access to specific departments and Schools	Schools such as Arts, Humanities/Soc Sciences
Admissions Action Security	Grants Admission Actions used to process a student's application and progress through the application process	"All" Admissions Action Security or security to specific Program Actions:
Program Action Security	Grants Program Actions used on Students	Can assign "All" Program Actions Security or security to

	student's Program/Plan page - identifies the status of the program – Active, Discontinued, or Completed.	specific Program Actions:

Application Center Security	Grants users access to Application Center by Institution	Values: W171- Academic Applicant W172 – Academic Applicant W220 – Academic Applicant
Recruiting Center Security	Grants users access to Recruiting Center by Institution	Value "PRSF" – Academic Prospect" UGRD career.
Campus Community 3C's Group Security	3Cs Comments, Communications and Checklists) are a flexible way to track and analyze correspondence, lists of requirements, and notes about the students, staff, and external organizations in the PeopleSoft database.	Users are assigned 3C's group security for the comments, communications, and checklists that a user needs.

	Comment Management– enables you to enter notes in the database about individuals, organizations, or events. **Communication Management**– enables you to manage the institution's incoming and outgoing contacts with students, prospects, recruits, staff, alumni, donors, and organizations. **Checklist Management**– enables you to create lists to track activities and dues dates, and identify their status at any time.	
Enrollment Security	Grants users enrollment security. This allows users to enroll students during the registration period. It controls when and who can enroll students.	Enrollment Security IDs: CNV Conversion RALL Registrar – All Access
Service Indicator Security	Provide or limit access to services for a student. Service Indicators can be holds that prevent a student from receiving certain services or positive indicators that designate special services to be provided.	A "hold" transaction on a student account. Service Indicators have service impacts such as Add Enrollment (do not add). Some Service Indicators have no impact and are for information only, others prevent enrollment, releasing a transcript, and/or issuing a refund.

	This functionality allows college's to protect information based on state and federal guidelines. **FERPA** (Family Educational Rights and Privacy Act) **Americans with Disabilities Act of 1990 HIPAA** (Health Information Privacy Accountability Act)	Row level security allows you to grant "Placement" and "Release" options for individual Student Groups per user.
Student Groups Security	Student Groups enables you to define groups of similar students at a high-level.	Scenario: Spokane Community College would to like to identify

	Creating groups of students enables you to track and use the students within a group for campus-wide processing, such as billing, academic advising, or financial aid awarding. Student group security defines the user's access to view or update student group data based on each of their academic institutions. If users are not setup with student group security, they will not have access to view or update student group information. Academic Institution security must be granted to a user prior to student group security being setup.	students who are physically handicapped and may need assistance evacuating in case of an emergency. SCC currently does not have a way to identify these students without violating their privacy. Student Services can now maintain a student group of physically handicapped students and secure visibility only to Campus Security.
Transcript Type Security	Grants a user access to transcript types	Types: Unofficial Transcript Official Transcript
Test ID Security	Grants users to Test Ids	Test IDs: ACPLC – ACCUPLACER ACT – ACT Assessment AP – Advance Placement ASSET – ASSET CLEP – College Level Examination Prg COMPS – COMPASS DSST – DANTE Standardized Subject Tst IB – International Baccalaureate IELTS – International English Language PTE – Person Test of English SAT – Scholastic Assessment Test

		TOEFL – Test of Engl as a Foreign Lang You can assign users to "all" test IDS or specific Test IDs.
Advisement Report Security	Grants user access to advisement reports Defines the user's access to advisement reports based on each of their academic institutions. Users can be setup for: -All access -access to specific report type Users not set up will have no access	Provides additional privacy for student information Restricts advisors to specific advisement reports
Population Update Security	The Population Update is a process that uses the Population Selection utility to update values in selected fields. Grants users access to Population Update records and fields for running processes with the Population Update functionality.	After choosing the records and fields to make available for update, set user security to identify who can update the records. This is a powerful tool; however it also has the potential to be dangerous. Population update should only be granted to the users that have had training and are experienced in creating queries.
Student Financials Security – row level		
Item Type Security	A transaction code. Item types are categorized as charges, payment, financial aid, refund and waiver.	Grants specific Item Type security to cashiers for posting charges and payments on student accounts.
HCM Row Level Security		
	Restricting Data to the Persons who are not authorized to see and also providing access to the data who are authorized to see is	Transaction Security Data is the data that is being secured. Certain transaction fields on a transaction data row are used to secure access to that row of data. The data in these

	called Data Security. Row level security prevents the user from being able to access data they are not allowed via the search page.	fields is called transaction security data. When the value of the transaction security data matches the value that a user can access (user security data), the system makes the entire row of data available to the user. See Diagrams 5.1. 6.1 7.1 for an example of HCM transactional data and security. Fields available for transaction security data:
Financials Row Level Security		
Row Level Security in PS Financials	To establish row level security, you must first decide the level that you want, which key fields to secure, and whether security will be defined through user IDs or permission lists. With row-level support, you can implement security to restrict individual users or permission lists from specific rows of data that are controlled by the following key fields:	Financials row level security is secured using a primary permission list that is attached to User Profiles.
	· Business Unit · SetID · Ledger (and ledger group) · Book · Project · Pay cycle · Planning Instance	
Other Security Roles needed to perform functions within the PeopleSoft applications.		
Query and Process group security		Query and Process Group roles are controlled by permission lists that are then attached to roles.

Query	The graphical tool for building on-line reports of information stored in the database.	Defines table row sets accessible for performing system queries.
Process Group	Grants users the ability to run processes in the system – can restrict based on job function.	
Process Monitor	All jobs that run in PeopleSoft are listed in the process monitor under your User ID.	Process monitor works with process scheduler to manage your nightly job stream as well as on-demand tasks. Process security gives users access to run processes within the PeopleSoft system.
Report Manager	Grants users access to the Report Manager	
Instance	A database is housed in an instance (environment)	Production Test Development
Security Matrix defined	Collection of navigation, menus,	1. Identify for each role the pages that the role has

	components, pages and actions for mapping to roles. Excel spreadsheet Rows - navigation, menus, components, and pages and actions Columns – lists the navigation: Folder, Menu Item/ Content Reference, Page Display Name, Security Menu, Security Component, Security Page, Action and the remaining columns represents the "role(s)" such as CTC_REGISTRAR. Identify the actions that can be performed on the component and page in the column under the role that you want to assign the page access to. Use letter codes to designate the action. For example: A for Add, C for Correction, U for Update/Display, UL for Update/Display All, and D for Display only.	access to and the actions that can be performed on those pages: Add, Update/Display, Update/ Display All, Correction, Display only. 2. Displays all the PS navigation available to a given group of roles. 3. Tool for designing managing user "role" and "row"- level security. 4. Based on Business Process Diagrams (BPD) for example, the BPDS answer: who does this function at your college or district or which department owns this task or function?

	5. User may have several roles depending on the hat(s) they wear.