PeopleSoft Security v8.9
Training Manual
1.0 Course Introduction

1.1 Objective
Developed specifically for PeopleSoft v8.9 Financials (FMS) functional end users, PeopleSoft Security v8.9 training quickly introduces students to the building blocks of PeopleSoft security. The goals of this class are achieved through a mixture of live PeopleSoft Security component walk-throughs and a hands-on exercise that allows students to apply security to a PeopleSoft FMS module as transactions are entered and processed.

1.2 Audience
The target audience is Functional end-users and/or Functional Project Team members. Please note that this is not a comprehensive class geared for Developers or Security Administrators.

1.3 Prerequisite
Intro to PeopleSoft v8.9 Financials Training

1.4 Duration
Two Days

1.5 Instructor Background
SpearMC Senior PeopleSoft Financials Consultant

1.6 Pre-class Items & Training Material
- SPEARMC Memo to Class and Expectations
- PeopleSoft Security Training Agenda
- PeopleSoft Security Training Manual
  - Technical: Not necessarily covered in this class – good future reference for tech users
  - Notes: Items of interest based on recent PeopleSoft v8.9 Security roll-outs
  - Discussion Points: Specific SpearMC points to discuss topic being covered
- PeopleSoft Security Training Exercise
- PeopleSoft Security Process Flow Example
- PeopleSoft Security Strategy and Considerations
2.0 Overview of PeopleSoft Security

PeopleSoft security in v8.9 uses a role-based security model. This is considered a security leading practice as it allows the flexibility and robustness to maintain the integrity of the system and its data.

The concept of decentralizing security is also supported in PeopleSoft, as it makes it more convenient for non-security administrators (e.g. super users, managers) to assign roles to end-users without exposing all security administration functionality. This course will cover the core components of PeopleSoft Security specifically geared towards non-security administrators.

A security definition refers to a collection of related security attributes that are created using PeopleTools Security. The three main PeopleSoft security definition object types are:

- User Profiles, Roles and Permission Lists

Each user of the system has an individual User Profile, which in turn is linked to one or more Roles. To each Role, you can add one or more Permission Lists, which ultimately control what a user can and can't access. So a user inherits permissions through the role.
The panel below (Figure 1) shows the Base Navigation Page for PeopleSoft Security.

Navigation: **PeopleTools > Security**
2.1 User Profiles Overview

A User Profile describes a particular user of the PeopleSoft system. This description includes everything from the low-level data that PeopleTools requires, such as Language Code, to application-specific data, such as the Table SetIDs a user is authorized to access within the PeopleSoft applications. User Profiles also maintain the Roles that are assigned to the user.

Technical: User Profiles are different from the application data tables, such as PERSONAL_DATA, that also store information about people. User Profiles are relevant when a user interacts with the system by logging in, viewing a worklist entry, receiving an email, and so on. Application data tables are involved with the core application functionality, such as payroll processing and expense sheet processing, not with system-wide user interaction.

2.2 Roles Overview

Roles are assigned to User Profiles. Roles are intermediate objects that link User Profiles to Permission Lists. Multiple Roles can be assigned to a User Profile, and you can assign multiple Permission Lists to a Role. Some examples of Roles might be Employee, Manager, Customer, and so on.

A Manager is also an Employee. Roles enable us to mix and match access appropriately.

Technical: There are two options when assigning roles; assign Roles manually or assigning them dynamically. When assigning roles dynamically, you can use PeopleCode, Light Directory Access Protocol (LDAP), and Query rules to assign User Profiles to Roles programmatically.

2.3 Permission Lists Overview

Permission Lists are lists, or groups, of authorizations that you assign to Roles. Permission Lists store Sign-on times, Page access, PeopleTools access, and so on.

A Permission List may contain one or more types of permissions. The more types of permissions in a Permission List the more modular and scalable your implementation.

A User Profile inherits most of its permissions through the roles that have been assigned to the User Profile.

Data permissions, or row-level security, appear either through a Primary Permissions List or a Row Security Permissions list.

Review / Q&A: How are the different agencies currently handling security? Start thinking about similarities and/or differences that currently exist vs. the PeopleSoft model.
3.0 Permission Lists

Permission Lists (Figure 2) are the building blocks of end user security authorizations. Before beginning to define User Profiles and Roles, you typically create our list of Permission Lists. When defining Permission Lists, consider each type of Role and User Profile to which they will be attached.

Important to Note: PeopleSoft comes delivered with many pre-defined Permission Lists. SpearMC recommends that SpearMC make use of as many of these permission lists as possible.

A Permission List may contain any number of the following permissions: (i) page permissions, (ii) signon times, (iii) process permissions, component interface permissions, and so on.

Important to Note: You will focus primarily on Page Permissions and Process Permissions for this class.

PeopleSoft Security is built off of the Permission List > Role > User Profile concept. Remember that a role may contain numerous permissions and a user profile may have numerous roles assigned to it.

Because permission lists are applied to users through roles, a user inherits all the permissions assigned to each role to which the user belongs. The user's access is determined by the combination of all of the roles.
Review / Q&A: Make sure you understand the concept of PeopleSoft Security. At a high-level think of Permission Lists as the component that allows a user what navigation is available to them and what process they can run.

Theoretically, you can create a Permission List tailored for each and every Role, and that Permission List could contain a permission of every category from General to Libraries. Alternatively, you can use a more modular or "mix-and-match" approach. This approach involves numerous, specific Permission Lists that you can add and remove to Role definitions. As a general rule, permission lists should be assigned to roles so that the common user has in between 10 to 20 lists.

Technical: When you set component permissions and your library permissions, there is a "View Content References" link that enables you to be able to view the content references pointing to a given component or script. PeopleTools automatically propagates changes to permission lists to the content references. When copying (cloning) a permission list, the content references associated with the copied permission list are also copied. Also, when deleting a permission list, the content references associated with that permission list are also removed.

Hands-on: Select the PeopleSoft delivered role for Voucher Entry and Correction (Figure 3).