

Security Strategy (T015)



Tom Gallagher

Chief Financial Officer



State of Florida Project Aspire

Security Strategy T015

Table of Contents

1.0	INTRODUCTION	2
1.1	DOCUMENT PURPOSE AND ORGANIZATION	2
1.2	DOCUMENT SCOPE	2
1.3	ASSUMPTIONS	2
2.0	SECURITY OBJECTIVES	3
3.0	ROLES	4
3.1	APPLICATION SOFTWARE LEADS AND ALTERNATES	4
3.2	SECURITY ADMINISTRATORS	4
3.3	DATABASE ADMINISTRATORS	5
3.4	SYSTEM ADMINISTRATORS	6
4.0	SECURITY GUIDELINES	7
4.1	OPERATING SYSTEM SECURITY	7
4.2	DATA SECURITY	7
4.3	USER SECURITY	8
5.0	PEOPLESOFT APPLICATION SECURITY	10
5.1	OVERVIEW	10
5.2	USER IDS	11
5.3	ROLES DEFINE PEOPLESOFT APPLICATION PRIVILEGES	12
5.4	PASSWORD MANAGEMENT	12
5.5	PASSWORD SELECTION	13
5.6	REQUESTING NEW OR MODIFYING USERS	14
5.7	ROW LEVEL SECURITY	15
5.8	PEOPLESOFT QUERY	15
5.9	PEOPLESOFT TREES	16
5.10	SINGLE SIGNON	16
6.0	INFRASTRUCTURE.....	18
6.1	DATABASE MANAGEMENT SYSTEM	18
6.2	OPERATING SYSTEMS	19
6.3	NETWORK	20
6.4	PHYSICAL SECURITY	21
6.5	WORKSTATIONS.....	22
7.0	CENTRALIZED AND DECENTRALIZED SECURITY.....	23
7.1	CENTRALIZED PEOPLETOOLS SECURITY	23
7.2	DECENTRALIZED PEOPLETOOLS SECURITY	23
7.3	CENTRALIZED APPLICATION SECURITY	24
7.4	DECENTRALIZED APPLICATION SECURITY	24
7.5	CONCLUSION AND RECOMMENDATIONS.....	24

1.0 INTRODUCTION

1.1 Document Purpose and Organization

This document discusses PeopleSoft security concepts that should be considered as Project Aspire is implemented. These concepts include but are not limited to end-user application security, database security, operating system security and remote access. The document also discusses strategies that can be used to secure the PeopleSoft system. It should be used as a reference to help plan, at a high-level, future security requirements within the PeopleSoft application. The initial sections of the document provide background and generalized recommendations concerning security. The PeopleSoft specific strategies and recommendations for Project Aspire are contained within section 7.5 Conclusion and Recommendations.

1.2 Document Scope

This document discusses security issues and presents a strategy for securing the Project Aspire PeopleSoft system. It is not intended to be a procedural document or an operational guide.

1.3 Assumptions

- The production configuration for security will not be finalized until the Application Software team completes their functional analysis/workshops and has a conceptual design.
- Oracle 9i will be the RDBMS used.
- Sun Solaris will be the primary server operating system. The PeopleSoft file servers will run the Windows operating system.
- At least one full-time Security Administrator will be assigned to Project Aspire.
- Project workstations will be Windows machines.
- Avoid modifications to delivered PeopleSoft application security.
- Avoid modifications to delivered PeopleTools security.
- PeopleSoft EPM security elements for Business Unit and SetID will be implemented consistent with that of PeopleSoft Financials application security.
- PeopleSoft Portal security provides for navigational access to content defined and controlled within the PeopleSoft Financials system. An individual user's access to actual information is restricted to the access identified for the user within the PeopleSoft Financials system.

2.0 SECURITY OBJECTIVES

This section details the objectives of the security strategy and further details the scope of the Project Aspire security effort. This includes the objects and components of the Project Aspire application and architecture that will be covered in this document.

In general, security must be established for two main reasons:

- To prevent accidental modification, deletion, or viewing of data. Typically, a user that is not familiar with the system could make a mistake that could affect the entire organization in a negative way, if restrictions to access are not controlled in some respect. It is also a priority to protect sensitive information from being accidentally discovered by the wrong parties.
- To prevent malicious interference or intrusions to the system. The more people that have access to the system, the greater the chances of this problem occurring. In a well-planned, controlled environment, the probability of a security breach diminishes. Excessive security procedures can become a burden to the end-user. A balance must be achieved to prevent unwanted access to those who are not authorized, while establishing easy to use procedures for access to the system for those who are authorized to use it.

System security will be addressed at multiple levels including the network, operating system, database and application levels.

3.0 ROLES

The project team roles and their respective responsibilities for ensuring the integrity of PeopleSoft security are outlined below.

3.1 Application Software Leads and Alternates

Application Software Leads are responsible for understanding the PeopleSoft Application modules under their control (i.e., General Ledger, Payables, etc.). For security purposes, each Application Software Lead owns the responsibilities, roles, and groups associated with access to system objects related to the application module for which they are responsible. Thus, the Security Administrator will ensure that the owning Application Software Lead has approved any change of access to a system object regardless of access mechanism (application, database, or server). If an individual requests access to objects that are owned by multiple Application Software Leads, then each Application Software Lead must approve the applicable request.

Application Software Leads administer and approve access to any system resource within their particular area, such as General Ledger, Payables, or Purchasing. The holder of this role also has the ability to create new responsibilities within individual applications. The Application Software Leads may also assist the Security Administrator with any of their tasks as they apply to their particular applications, such as defining Role authorizations or defining Role assignments to operators.

Application Software Leads are accountable to the management teams within their own organizations. The procedures stated in this strategy are open to review and criticism at the request of the Application Software Leads. These leads will be able to respond to individual's needing various access privileges by formally submitting requests (User Security Add/Modify Form) within their immediate domain of control.

3.2 Security Administrators

The Security Administrators maintain overall PeopleSoft security. They are the first individuals to receive requests for the addition and/or termination of User ID's. They are also the central point for access requests for existing IDs that are not within the domain of control offered by Application Software Leads. This administrator will log and file copies of the requests, ensure the appropriate resources are informed of needed actions, and inform users when the request is complete.

The Project Aspire Security Administrator is responsible for this document, ensuring that all users abide by the specifications contained within this document, and routing access requests to the appropriate resources. The Security Administrator may be required to approve certain actions prior to altering system access privileges, as listed later in this document. The Security Administrator is the chief executor of security of the PeopleSoft Application suite and any related resources. Thus, if any of the listed policies or guidelines contained within this document are unclear, the Security Administrator should be consulted for the proper interpretation.

The Security Administrator and their backups can grant any level of access or responsibility definition for PeopleSoft Applications. This responsibility includes providing limited administrative capabilities to Application Software Leads. This is a guarded position and must be protected as such. This role provides the ability to administer the rights to any menu, component, page or tool within any PeopleSoft Application module. The activities performed within this role should be reviewed and audited to ensure applicability by internal audit.

At least one person should be named as a full-time Project Aspire Security Administrator. Other staff can help in this role part-time. The Application Software Teams will develop a security matrix that describes what access each end-user needs. The Security Administrator is responsible for working with the Application Software Leads to ensure that the end-user security they have designed is implemented.

Periodically, the Security Administrator should perform a security audit. This should include reviewing PeopleSoft security and also include changing passwords to sensitive accounts such as Unix and Windows server passwords and database passwords. It should also include looking for unencrypted passwords in configuration or interface files. For example, the application server configuration files contain the database password. Encryption is available for this password and is recommended but is not required.

3.3 Database Administrators

The Database Administrator (DBA) is responsible for ensuring that the database is adequately configured and installed to support the entire PeopleSoft Application suite. These tasks include: capacity planning and management, tuning, installation, ensuring referential integrity, ensuring adequate database design techniques are used to create new applications or make changes to existing applications, etc. The DBA controls the security of the database for individuals wishing to access the database via avenues other than the core PeopleSoft Applications (i.e., third-party query tools).

Thus, the DBA and his backups can grant any level of access to any database object. This responsibility includes providing limited administrative capabilities to other administrators. This is a guarded position and must be protected as such. The activities performed within this role should be reviewed and audited to ensure applicability.

The DBA and his backups are the only resources that can have the ALTER USER privilege on the database. The procedures listed in this document govern the mechanisms others use to request alteration of user privileges. Users can execute the ALTER USER command to change their password and no special privileges are required, but this is the only use of this command that should be permitted to the users.

The DBA is the primary person responsible for ensuring that adequate distribution and control of systems resources exists to prevent data contamination due to resource exhaustion.

3.4 System Administrators

System Administrators are the security and functional equivalent of the Security Administrator, and DBA for the controlled access to file and application servers. Therefore, these individuals can grant access to any of the server objects (i.e., the ability to add, delete, and change files; add, create and delete directories, execute applications, compile and execute C programs, etc.). This responsibility includes providing limited administrative capabilities to other individuals that have been designated to help disperse this responsibility, as dictated by need and management. This is a guarded position and must be protected as such. The activities performed within this role should be reviewed and audited, by internal audit, to ensure applicability.

4.0 SECURITY GUIDELINES

This section describes how different layers of the security architecture interact and what security layers the Project Aspire team will be responsible for.

4.1 Operating System Security

This section describes the role that operating system security will play in Project Aspire and how it will interact with PeopleSoft application security.

The following security issues apply for the operating system environment executing PeopleSoft at Project Aspire:

- The DBA has the operating system privileges to create and delete files.
- The database users do not have the operating system privileges to create or delete files related to the database.

4.2 Data Security

This section describes what processes and policies are in place, above PeopleSoft Application Security, to protect Project Aspire data.

Data security includes the mechanisms that control the access and use of the database at the object level. A data security policy governs how users are provided access to specific schema objects, and the specific types of actions allowed on those objects. The policy should be flexible enough to permit adequate management of security without continuous policy change in response to organization changes. For example, user SCOTT can issue SELECT and INSERT statements but not DELETE statements using the EMP table.

The level of security deemed necessary to access the data within the database will determine the data security policy. For example, it may be acceptable to have little data security in a database when one wishes to allow any user to create any schema object, or grant access privileges for their objects to any other user of the system. Alternatively, it might be necessary for data security to be tightly controlled when the Database or Security Administrator is the only person with the privileges to create objects and grant access privileges for objects to roles and users.

Overall data security should be based on the sensitivity of data. The DBA can build views to provide limited access to tables by not making particular columns of associated tables available. These limited “views” of the data can then be granted to the appropriate roles.

4.3 User Security

This section describes how PeopleSoft application security will impact the end-user.

Most individuals access the database will do so via the PeopleSoft Application modules. Thus, the guidelines contained in the **PeopleSoft Application Security** section below apply to most users. For those individuals that can access the database outside of the PeopleSoft Application suite, the following guidelines must be enforced:

1. All users must be authenticated at the database level.
2. Only DBAs may have the capability to connect to a database with administrator privileges.
3. Whenever an individual attempts to connect to a server using a password, PeopleSoft encrypts the password before sending it to the server. If the connection fails and auditing is enabled, the failure is noted in the audit log. PeopleSoft then checks the appropriate login value. If it is set to FALSE, PeopleSoft attempts the connection again using an unencrypted version of the password. If the connection is successful, the connection replaces the previous failure in the audit log, and the connection proceeds. To prevent malicious users from forcing PeopleSoft to re-attempt a connection with an unencrypted version of the password, the appropriate values must be set to TRUE.

4.4 Application Developer Security

This section describes the permissions Project Aspire developers will have to various PeopleSoft environments.

Database application developers are unique database users who require special groups of privileges to accomplish their jobs. Unlike end-users, developers need system privileges, such as CREATE TABLE, CREATE PROCEDURE, and so on. However, only specific system privileges should be granted to developers to restrict their overall capabilities in the database.

Application development is restricted to development and test databases and not allowed on production databases. This restriction ensures that application developers do not compete with end-users for database resources, and that they cannot detrimentally affect a production database. Developers that wish to get access to objects in the production database must obtain the Application Software Leads approval via the **User Security Add/Modify Form**.

The development manager will coordinate with administrators to define roles to manage the privileges required for each type of application developer. For example, a typical role named AP_APPLICATION_DEVELOPER might include the CREATE TABLE, CREATE VIEW, and CREATE PROCEDURE system privileges for tables that are shared between functions and tables

preceded by “AP_”, but not any other tables. Consider the following when defining roles for application developers:

- CREATE system privileges are usually granted to application developers so that they can create their own objects. However, CREATE ANY system privileges, which allow a user to create an object in any user's domain, are not usually granted to developers. This restricts the creation of new objects only to the developer's user account.
- Object privileges are rarely granted to roles used by application developers. This is often impractical because granting object privileges via roles often restricts their usability in the creation of other objects (primarily views and stored procedures). It is more practical to allow application developers to create their own objects for development purposes.

While application developers are typically given the privileges to create objects as part of the development process, DBAs must maintain limits on what and how much database space can be used. For example, as the DBA, one would specifically set or restrict the following limits for each application developer:

- The table spaces in which the developer can create tables or indexes.
- The quota for each table space accessible to the developer.

5.0 PeopleSoft Application Security

This section describes, at a high level, how PeopleSoft decentralized security and Agency\Business Unit security Application Security functions and how it will be implemented under Project Aspire.

5.1 Overview

PeopleSoft delivers advanced application security features that ensure your organization's data is only available to the appropriate end-users. PeopleSoft security is composed of PeopleTools security and application security.

PeopleTools security tools are used to control access to most of the PeopleSoft system. PeopleTools security includes items such as the ability to logon to the PeopleSoft applications, access to specific pages and access to specific processes.

Application security includes controlling access to specific business units, table sets (SetIDs), projects, etc. For those areas not covered by the PeopleTools security tools, application-specific security tools are available.

Together these security tools provide a comprehensive application security framework that allows you to restrict users to specific pages, development objects, batch processes, and data. You can also allow users to access the system only during specific days or times, and allow them to access specific database tables, rows of tables or specific queries. PeopleTools security is normally centrally controlled by the project's infrastructure group. Application security is normally centrally controlled by the project's functional groups.

PeopleSoft implements security through objects such as User Profiles, Roles and Permission Lists. Permission Lists control what a user can and cannot access. Permission lists are assigned to Roles and Roles are assigned to User Profiles. In this way PeopleSoft provides a modular way to efficiently and effectively apply application security.

Each PeopleSoft end-user is assigned a unique User Profile or User ID and password so that they can access the system. Often there are many users with similar access requirements. PeopleSoft security allows you to group these users. This makes maintaining PeopleSoft security much easier.

It is important to identify PeopleSoft end-users with similar responsibilities and to group them into Roles. For example, users should be grouped first by the PeopleSoft application they will need to access. Keep in mind that some users will need access to multiple applications. Then within each application, group users into Roles. For example, these users could be categorized as clerks, super users, supervisors, managers, etc. Then determine what type of access each group requires. Generally a supervisor would have much greater access than a clerk.

In more detailed terms, some users might only have the ability to sign-on to the system during specific days or hours, or be limited to specific pages, or be limited to which tables or rows of data they can access, or be limited to which processes they can run.

The Application Software teams will work with the State agencies to develop a detailed application security plan. Then they will forward the appropriate parts of that plan to the Security Administrator for input into PeopleTools security. The remaining parts of the detailed security plan will be implemented by the application software teams and/or the various State agencies.

In most cases, there will be situations where there is a need to copy security information from one database to another. Typically, this should be done as part of an upgrade or to transfer security information from the production environment to the development or testing environment. To do this, PeopleTools provides a set of Data Mover (DMS) scripts designed to export and import the security information. The provided scripts transfer user profiles from a source to a target database.

5.2 User IDs

This section describes the process of managing Project Aspire User IDs.

A PeopleSoft User ID is the logon name that your PeopleSoft end-users will need to gain access to the PeopleSoft system. A User ID is the key to a User Profile. For the purposes of this document, a User ID and a User Profile have almost the same meaning. A User ID is paired with a PeopleSoft operator password. A PeopleSoft Security Administrator administers the ID and password within the PeopleSoft application. Access to the PeopleSoft objects such as Pages, Records, Menus, etc. is controlled by granting access to those objects to a User ID.

An individual User ID will be created for each individual requiring access to the PeopleSoft system. This provides the ability to maintain clear audit trails of individual activity. Thus, unique and independent User ID's help support accountability. Each User ID will be assigned to responsibilities defined within the PeopleSoft Application, roles defined for the database, and groups on the database server and/or file servers. These responsibilities and groups provide for controlled access to system resources. The individual components will be discussed later. Thus, User ID's will be deleted and their rights modified as individuals change their roles within the corporation.

User Profiles can contain up to 30 characters. The name cannot contain a comma or a space. The User Profile PPLSOFT is reserved by PeopleSoft.

A report or query should be developed to alert the Security Administrator when User IDs have not been utilized within a specific number of days. This helps to ensure that accounts for terminated employees are not left active.

5.2.1 User ID Naming Convention

PeopleSoft User IDs can be up to 30 characters in length. However, User IDs are normally restricted to 8 characters to make them easier to use. Typically a naming convention is established. For example, User IDs might consist of the first 7 characters of a user's last name plus the first character of his first name.

For example, John Anderson would have JANDERSO as his User ID. If there are duplicate, non-unique User ID's, then the last character of the User ID would be dropped and a numeric character from 1 to 9 would be added. For example, John Anderson would then have JANDERS1.

5.3 Roles define PeopleSoft Application Privileges

This section describes the concept of PeopleSoft Roles and describes how and why it is a central concept to understanding PeopleSoft application security.

In PeopleSoft one can assign Roles to User Profiles. Roles are intermediate objects that link User Profiles to Permission Lists. One can assign multiple roles to a User Profile and multiple Permission Lists to a Role. Some examples of Roles might be Employee, Manager or Vendor.

Permission Lists are lists, or groups, of authorizations that you assign to Roles. Permission Lists store such things as Sign-On times, Page access and PeopleTools access. A Permission List might contain multiple types of permissions.

A User Profile inherits most of its permissions through the roles that have been assigned to the User Profile. However, there are a few Permission Lists that are applied directly to a User Profile.

User IDs, Roles and Permission Lists can be created, modified or deleted through the online PeopleSoft system.

5.4 Password Management

This section describes how PeopleSoft passwords should be managed.

PeopleSoft offers several features regarding password management. These features include the ability to set passwords so that they never expire or expire in a specified number of days. When a password expires, the user is forced to choose a new password. PeopleSoft also provides the ability to send warning messages to users to let them know that their password will expire soon.

Some other features include the ability to allow, or disallow, an end-user's password to match their User ID, to lock an account after a specified number of unsuccessful logon attempts, to set a minimum password length and to specify a required number of special characters or digits.

Collectively these features provide the ability to easily implement a customized password management policy that reduces the chance of passwords being compromised but still allows passwords to be managed.

The minimum password length should be set to eight characters long. Eight provides an acceptable level of security without making the password unmanageable.

5.5 Password Selection

Perhaps the most vulnerable part of any computer system is the account password. Any computer system, no matter how secure it is from network or dial-up attack can be fully exploited by an intruder if they can gain access via a poorly chosen password. The following are the Project Aspire guidelines for the selection of passwords:

- **DO NOT** use your User ID name in any form (as-is, reversed, capitalized, doubled, etc.)
- **DO NOT** use your first, middle, or last name in any form
- **DO NOT** use your spouse's or child's name
- **DO NOT** use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- **DO NOT** use a password of all digits, or all the same letter
- **DO NOT** use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words
- **DO** use a password with mixed-case alphabetic
- **DO** use a password with non-alphabetic characters (digits or punctuation)
- **DO** use a password that is easy to remember, so you **DO NOT** have to write it down
- **DO** use a password that you can type quickly, without having to look at the keyboard

Methods of selecting a password, which adhere to these guidelines, include:

- Choose a line or two from a song or poem, and use the first letter of each word.
- Alternate between one consonant and one or two vowels, up to seven or eight characters. This provides nonsense words, which are usually pronounceable, and thus easily remembered.

- Choose two short words and concatenate them together with a punctuation character between them.

5.6 Requesting New or Modifying Users

This section describes the process for requesting new user additions to the system and modifying the Roles existing end users have in the system.

When there is a need to add new users, a formal request must be made to the Security Administrator. This request should include details about what that user needs to access. Typically if this user can be modeled after an existing user, that makes the addition much easier for the Security Administrator. PeopleSoft provides the ability to copy an existing user's profile to a new user thus, saving time and effort when creating new users. To create, modify or delete a user, a form should be completed and forwarded to the Security Administrator. The following steps outline a sample scenario.

1. On the User Security Add/Modify Form enter the requester's name. This is the person that will be notified when the requested action(s) are completed.
2. Enter the requester's department name.
3. Enter the date by which the requested actions need to be accomplished. Allow at least one day for completion. If the requested actions are necessary within less than one day, then complete the request form and contact the Security Administrator directly to negotiate the feasibility of meeting the requested deadline. If the Operations staff determines that the requested actions can not be completed by the requested deadline, they will inform the contact and/or the requester and establish a realistic deadline.
4. If or when known, enter the date until which the User ID needs to remain effective. This date is useful for two primary purposes. First, this would permit the submission of a "User Security Add/Modify Form" to terminate access for a User ID by a specified date in advance of the actual date rather than subsequent to the date. This enables deletion as near to the termination point as possible without hampering the individual's work. Secondly, this allows for requesting a temporary User ID or special access for an existing User ID that is only available for a set timeframe.
5. Select the type of request (New, Change, or Terminate). For terminations, requests should be submitted as early as possible to permit prompt deletions.

Sample Security Check List for New/Modify Users

1. Receive completed User Security Add/Modification Form
2. Identify User Setup – Roles from Application Development Leads
3. Add/Modify User ID

4. Update Operator Preferences
5. Workflow Role User Setup/Modification
6. Notify Admin to setup/Modify Requestor and Buyer
 - a) Also Need to update Approvers to have authority to approve new/modified user's requisitions if applicable
7. E-mail new user with User ID and generic password
8. Sign off on submitted forms
9. File forms in Security Binder

5.7 Row Level Security

With row-level security, users can have access to a table without having access to all rows on that table. This type of security is typically applied to tables that hold sensitive data. For example, Project Aspire requirements may dictate that end-users have the capability to review Project data for their area within an agency but not for the entire agency.

PeopleSoft applications implement row-level security by using a SQL view that joins the data table with an authorization table. When a user searches for data in the data table, the system performs a related record join between the view and the base table rather than searching the table directly. The view adds a security check to the search, based on the criteria you've set up for row-level security. For example, to restrict users to seeing Project data for their area, the view would select from the underlying tables just those rows where the Business Unit and Project matches the user's authorized Business Unit and Project values.

PeopleSoft applications are delivered with built-in, row-level security functions that are tailored to specific applications. For example, in PeopleSoft Financials you can use security views to determine who has access to which Business Units, SetIDs, Ledgers, Books and Projects.

5.8 PeopleSoft Query

Query is a PeopleTool that helps you build SQL queries to retrieve information from your application tables. For each Query user, one can specify the database tables a user is allowed to access when building and executing queries. In PeopleSoft it can be done by creating Query Access Groups in PeopleSoft Tree Manager, and then assigning users to those groups with Query Security. Keep in mind that Query security is enforced only when using Query; it doesn't control runtime page access to table data.

Thus an end-user can be restricted from running a particular query or can be restricted to viewing only specific rows in the query result set.

PeopleSoft also allows you to decide whether you want to let users create queries and then execute them or restrict users to executing existing queries. In the production environment, the ability to create queries should be limited. Query access should be limited because inefficient queries can greatly affect the performance of the production environment. Most users should only be allowed to execute existing queries that have been tested in development and test environments.

Query security is integrated with PeopleTools security.

5.9 PeopleSoft Trees

PeopleSoft delivers application functionality called trees that allow you to represent your data graphically to show a hierarchy. Other parts of the system can use the trees that you've defined for hierarchical information—for reports, ChartField combination editing, OLAP, summary ledgers, or security. One can update trees with specifically designed tools, and the changes are then automatically applied throughout the system.

One can use PeopleSoft Object Security to impose restrictions on trees. Users can have access to an entire tree, or to part of a tree. Access can be read-only as well.

The Tree Manager PeopleTool is used to administer Tree security.

5.10 Single Signon

PeopleSoft supports single signon within PeopleSoft applications. Within the context of the PeopleSoft system, single signon means that after a user has been authenticated by one PeopleSoft application server, that user can access a second PeopleSoft application server without entering an ID or a password. Although the user is actually accessing different applications and databases, the user navigates seamlessly through the system.

After the first application server/node authenticates a user, PeopleSoft delivers a web browser cookie containing an authentication token. The PeopleSoft Internet Architecture (PIA) uses web browser cookies to store a unique access token for each user after they are authenticated initially. When the user connects to another PeopleSoft application server/node, the second application server uses the token in the browser cookie to re-authenticate the user behind the scenes so they don't have to complete the signon process again.

Single signon is critical for PeopleSoft portal implementations because the portal integrates content from various data sources and application servers and presents them in a unified interface. When the users signon through the portal, they always take advantage of single signon. Users need to signon once and be able to navigate freely without encountering numerous signon screens. Because single

signon is so integral to the portal, you always need to configure it before deploying a live portal solution.

In the Project Aspire configuration, end-users will signon to an Enterprise Portal database. From there they can select a link that will automatically sign them on to either the Financials or Enterprise Performance Management (EPM) databases.

The browser cookie is an in-memory cookie and is never written to disk. The cookie is also encrypted to prevent snooping and digitally signed using a check sum to prevent tampering.

6.0 Infrastructure

This section describes strategies for configuring the overall infrastructure to deal with security concerns including specific areas such as database access, network access, worms, viruses and hacking.

6.1 Database Management System

In addition to data security provided by PeopleSoft, the security features of the Oracle RDBMS should be implemented. At a high level database security includes controlling which users can logon to the database and which privileges those users will have once they log on successfully. Database security also includes controlling access to specific tables or views and controlling access to Oracle administrative functions.

A DBA should be assigned to control access to the Oracle environment. This person must be technically proficient with the Oracle 9i RDBMS.

SQL Plus provides back-end access to the Oracle database. Therefore access to this powerful tool should be monitored and limited to only those individuals with a genuine need. Users requiring read only access to PeopleSoft tables can easily be granted such access. Update access should only be granted where warranted. Access can be completely restricted by disallowing signon.

Oracle 9i RDBMS is delivered with several standard user ids and passwords. The delivered passwords are generally known to those people that have worked with Oracle products. Therefore the passwords for the sys and system user ids should be changed after each database is created. Also, the use of these two user ids should be limited to key personnel.

The Oracle Unix account is established with the Oracle RDBMS product install. This account is used to install the product, apply maintenance and perform administrative functions like starting or stopping a database. Therefore the use of this account should also be tightly controlled.

Each PeopleSoft database will consist of numerous Unix files. These files, which include files such as database, redo and control files, should have the proper Unix permissions assigned to them so that only authorized users would be able to access them. With the exception of the DBA and/or Unix System Administrator, no one would ever require direct access to these files. Access would generally come from within the PeopleSoft application.

Database backups provide a mechanism for recovering your organization's data. These backups should be secured so that they remain available in case they are ever needed.

In addition to allowing end-users to update PeopleSoft databases through the online web pages, PeopleSoft provides a few other ways to update the databases. It is very important to be aware of these means so that they can be secured. SQRW and Data Mover are two other tools that can be

used to update the PeopleSoft database. Under normal system operation, both of these can execute SQL commands and don't necessarily provide an audit trail. The Project Aspire infrastructure team should become familiar with these tools and implement means to control their use. Access to both of these tools can be restricted completely by disallowing signon.

6.2 Operating Systems

This section is concerned with controlling access to the Solaris and Windows servers. Solaris will be used as the operating system for most of Project Aspire's servers. The Windows operating system will be used for the remaining servers.

It is important to keep current on operating system maintenance, especially when this maintenance deals with closing potential security vulnerabilities.

On Solaris, use of the root account should be very tightly controlled. This account should also be used only when needed. Because this account is so powerful, misuse of the root account could have devastating effects on the system. Similarly on Windows, use of the administrator account should also be tightly controlled for the same reasons.

Carnegie Mellon University maintains a very useful website with information concerning both Solaris and Windows security vulnerabilities. It can be found at <http://www.cert.org>.

All open ports will require justification. Where possible, port encryption via a secure method such as SSL, SSH or IPSEC will be used for communication.

Both internal and external port scans of all systems should be performed periodically.

All privileged access on Unix will occur through SUDO. Non-System Administrators will only be given SUDO access judged safe by the administrators. Any other root level access will occur with the assistance of a Systems Administrator.

File Systems

A series of PeopleSoft directories collectively known as the PS_HOME directories will exist on each Unix and Windows server. These directories contain all of the PeopleSoft batch programs such as SQR, COBOL and Crystal programs, SQL scripts as well as other files. Care must be taken to ensure that the correct version of each program exists in the appropriate directory at all times. Therefore write access to these directories should be limited to the infrastructure team so that control can be maintained.

There will be times when developers will have legitimate needs to write to the batch program directories on various servers but these times will be rare. In most of these cases, specific directories

can be created for the developers so that their code can be isolated to minimize its impact in the case of a problem.

Separate PS_HOME file sets should exist for each database environment. On Unix these directories should be tied to unique Unix accounts to allow their use to be tightly controlled.

System Logs

The Solaris Syslog is a centralized logging facility that provides different classes of events that are logged to a log file, as well as providing an alerting service for certain events.

The Solaris Syslog log files should be examined regularly. All auth notices should be logged and a cron job should be run every night to filter the results for a review in the morning.

Windows provides a similar event logging facility. Both the Unix and Windows system event logs should be reviewed regularly. Special attention should be paid to events such as unauthorized access, repeated unsuccessful attempts to sign on and logon attempts after normal business hours.

System logs should be written to a secure central server.

6.3 Network

Network security deals with controlling user access to the network's shared hardware and software resources. Several network issues and approaches are discussed in this section.

Firewalls

Firewalls provide a method for implementing security policies designed to keep a network secure from intruders. They range from fairly simple solutions to extremely complex solutions. A firewall can be a single router that filters out unwanted packets or may comprise a combination of routers and servers, each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate an organization's public Web server from its internal network.

Project Aspire should include firewalls as part of the overall system architecture.

DMZ

A DeMilitarized Zone (DMZ) provides a middle ground between an organization's trusted internal network and an untrusted external network such as the Internet. The DMZ is a subnetwork that may sit between firewalls or off one leg of a firewall. Organizations typically place their Web, mail and authentication servers in the DMZ.

Project Aspire should incorporate the use of a DMZ in the overall architecture. All systems, whether inside the firewall or in the DMZ, should be secured to the same standards.

Viruses

Viruses are software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. The effect of a virus can range from a minor nuisance to a major problem that destroys data or denies service to users.

Worms

Worms are destructive programs that replicate themselves throughout disk and memory, exhausting a computer's resources and eventually bringing the system down.

Spyware

While much effort has been made excluding unwanted input to the internal network, less attention has been paid to monitoring what goes out. Spyware are applications that keep track of your habits and send those statistics to a Web site.

Hackers

Hackers are people who attempt to gain unauthorized access into a computer system. Their motives can range from mischief to fraud to the destruction of an organization's data. Hackers typically gain access to a system by decoding passwords of legitimate users or by taking advantage of vulnerabilities in a software product.

Commercial products are available to combat viruses, worms, spyware and hackers and to minimize their effects. Project Aspire should incorporate one or more of these tools into the overall security plan.

6.4 Physical Security

Physical Security refers to the method used to control physical access to the servers and other infrastructure components by unauthorized personnel.

Servers and other infrastructure components that are accessible to unauthorized persons present an increased security threat. These components can easily be altered, destroyed or even physically removed. This concern also applies to peripherals such as tapes and printed reports.

Servers and other infrastructure components should be located in a secure room. Access to that room should be limited to the appropriate infrastructure team members. Access to the room should

be secured by key or security card. This will help to minimize the chances of a component being taken offline or being stolen or misused.

Tape backups should be stored in a secure place. They should be accessible in the case of an emergency but should only be readily available to specific infrastructure personnel.

Both the infrastructure components and backups should be stored at climate controlled sites. They should also be rotated to an off-site location as part of a disaster recover plan.

6.5 Workstations

Workstations provide another means of introducing viruses or worms into your environment. Therefore all workstations should periodically run virus detection software and should be kept current on Windows maintenance dealing with security vulnerabilities.

Screen saver passwords should be used to control access to the PeopleSoft system in case the user leaves his machine unattended for a long period of time.

The PeopleSoft application also provides the ability to log users off the system after a specified period of inactivity. This feature should also be implemented by the Project Aspire team.

7.0 Centralized and Decentralized Security

This section provides an overview of centralized and decentralized security and the security related goals of Project Aspire. During the Business Process Workshops, the Application Software teams will identify and confirm security considerations and requirements as the conceptual design is formulated. These considerations and requirements will serve as input to the design and implementation of security with regards to PeopleTools security and PeopleSoft application security.

For this section of the document, it is important to keep in mind the distinction between PeopleSoft PeopleTools security and PeopleSoft application security as stated in Section 5 of this document which is:

PeopleTools security includes items such as the ability to logon to the PeopleSoft applications, access to specific pages and access to specific processes. Application security includes controlling access to specific business units, table sets (SetIDs), projects, etc.

7.1 Centralized PeopleTools Security

PeopleSoft PeopleTools security has historically been designed and delivered as a centralized model. PeopleTools security is typically administered by members of a centralized IT staff. This centralized model provides a relatively simple to implement, proven solution. Since the delivered PeopleSoft security model has been thoroughly tested by PeopleSoft and has been implemented by numerous clients, there is little risk with this approach. PeopleSoft also provides PeopleBooks and Upgrade documentation to make maintaining PeopleTools security easier.

With the centralized PeopleTools security approach, all security requests are sent to a centralized IT staff. These requests typically include items such as creating and removing logon IDs and granting a user access to a specific page or process.

7.2 Decentralized PeopleTools Security

Some organizations might find that the centralized PeopleTools security model does not meet their needs and find that they want to decentralize or distribute administration of security. Decentralizing security gives areas other than IT more direct access to the PeopleTools security administration. This can result in less dependence on the centralized IT staff and faster turnaround for security-related requests.

Recent releases of PeopleTools (8.4x) have provided new functionality for distributing the creation and maintenance of user profiles (User IDs) to a managerial or departmental level. This new functionality provides the ability for an agency security administrator to create and maintain User IDs within the agency perspective without impacting other agencies. As this is a newly released function, it should be thoroughly tested to ensure that it does provide adequate controls and does not compromise overall system security and integrity.

Depending on the specific functions that are to be decentralized, decentralized security can add complexity to the implementation. For example, staff may need to be retooled, additional configuration and customizations may be required based on what is decentralized and system performance and integrity can be affected by customizations. A Security Proof of Concept (POC) should be performed to ensure any decentralized aspects of the security solution works as planned and meets the operational needs of the enterprise without compromising overall system integrity.

A detailed analysis and design must be performed. The specific functions to be decentralized must be identified and documented. It is generally a good idea to only decentralize those functions that affect a particular agency. Functions that affect all users regardless of agency such as stopping or starting application servers and process schedulers are best kept centralized.

7.3 Centralized Application Security

PeopleSoft application security has historically also been delivered as a centralized solution. This model is typically administered by members of the Application Software team. Application security can be activated at the User ID level or at the Permission List level. For Business Unit security, the administrator grants a specific user or Permission List access to specific Business Units. This same process would be repeated for Table Sets (SetID), Projects, etc.

7.4 Decentralized Application Security

Some organizations might find that the centralized application security model does not meet their needs and find that they want to decentralize application security. Decentralizing application security can give individual agencies more direct access to the application security administration. This can result in less dependence on the centralized application software team and faster turnaround for application security-related requests.

To decentralize application security, each agency's security administrator would be granted access to the PeopleSoft pages that allow one to administer application security only within the agency.

As with decentralizing PeopleTools security, a detailed analysis and design must be performed. A Proof of Concept would probably not be needed here since this is not as complicated as decentralizing PeopleTools security, but detailed testing should still be performed to ensure that the decentralized security solution is working as planned.

7.5 Conclusion and Recommendations

PeopleSoft Security Administration tends to be a centralized model within most organizations. The recent releases of PeopleSoft 8.4+ and the PeopleSoft Internet Architecture (PIA) now allow for decentralizing some administrative functions. Decentralizing security administrative functions allows for organizations (agencies) to administer security with some autonomy instead of relying on a centralized support organization.

Centralized security administration, by its nature, provides a central control point and allows for simplified coordination of security decisions. Decentralized security administration distributes the administrative access out to each organization requiring additional controls and coordination across all organizations in order to prevent or minimize impacts related to system functionality, integrity or performance.

The Project Aspire strategic objectives related to centralized and decentralized administration of security are to:

- Provide a balance of both centralized and decentralized security administration whereby as many security administrative functions are distributed to the agencies as possible without adversely impacting the overall system functionality, integrity or performance.
- Provide autonomy to agencies in administering their own security with proper controls in place to avoid impacting to other agencies.
- Avoid modifications to the delivered PeopleTools security administration other than setup and configuration aspects such as Roles, Permission Lists and setup of the Distributed User Profile component.
- Avoid modifications to the delivered PeopleSoft application security other than setup and configuration aspects or restricting access (via PeopleTools security) to individual pages within PeopleSoft application security.
- Utilize delivered setup and configuration capabilities in PeopleTools security and PeopleSoft application security to implement any decentralized (distributed) security.

Based on the strategic objectives, the specific recommendations for Project Aspire for administration of different functional aspects of security are:

Access Function	Type of Security	Recommended Administration	Accomplished by Configuration or Customization	Details	Concerns
User Profiles Creation and Maintenance	PeopleTools	Centralized	Configuration	Intended for system (wide) administrators and allows for providing access to all aspects of PeopleSoft and PeopleTools for all Aspire users.	Developing and standardizing the processes for all agencies to request and have user profiles created and updated.
Permission Lists Creation and Maintenance	PeopleTools	Centralized	Configuration	Setup and maintenance of enterprise wide security model. User access to Permission Lists is via Roles.	Enterprise wide model with exceptions as required addressing specific agency needs.
Roles Creation and Maintenance	PeopleTools	Centralized	Configuration	Setup and maintenance of enterprise wide security model. User access to Roles is accomplished in either User Profiles or Distributed User Profiles.	Enterprise wide model with exceptions as required addressing specific agency needs. Care and consideration should be given to the design of Roles since the Role is a key part of Workflow setup and controlling the Workflow process.

Access Function	Type of Security	Recommended Administration	Accomplished by Configuration or Customization	Details	Concerns
Tree Manager Enterprise Wide Access	PeopleTools	Centralized	Configuration	Basic Tree access and setup.	Limit access to users with centralized or system wide business responsibilities (setup).

Access Function	Type of Security	Recommended Administration	Accomplished by Configuration or Customization	Details	Concerns
Tree Manager Nodes Enterprise wide	PeopleTools	Centralized	Configuration	Individual nodes on the Tree can be secured using elements such as SetID along with PeopleSoft Object Security.	Dependent upon application design of SetIDs providing controls unique to an agency.
Tree Manager Agency Specific	PeopleTools	Centralized	Configuration	Basic Tree access and setup.	Limit access to users with centralized or system wide business responsibilities.
Tree Manager Nodes Agency Specific	PeopleTools	Decentralized	Configuration	Individual nodes on the Tree can be secured using SetID along with PeopleSoft Object Security. Allow for node creation and setup below root node.	Agency personnel will have full Tree access below the root node. Secured using agency specific SetID which will prevent agencies from affecting other agency's trees.
Business Unit Setup and Access	Application	Centralized	Configuration	Creation and management of the system's Business Units.	Limit access via Roles / Permission Lists to users with centralized or system wide business responsibilities (setup).
Assignment of Default Application Security	PeopleTools	Decentralized	Configuration	Implemented within User Profiles and Distributed User Profiles by designating a default Permission List that has been associated to a specific Business Unit in Application Security.	Setup of the Permission List should be Centralized.
SetID	Application	Centralized	Configuration	Creation and management of the system's SetIDs	Limit access via Roles / Permission Lists to users with centralized or

Access Function	Type of Security	Recommended Administration	Accomplished by Configuration or Customization	Details	Concerns
				system's SetIDs.	Lists to users with centralized or system wide business responsibilities (setup).
Projects	Application	Decentralized	Configuration	Access controlled by agency Business Unit.	
Chartfields Enterprise Wide	PeopleTools	Centralized	Configuration	PeopleTools Security and Application Security.	Enterprise wide chartfields will be maintained centrally. Agencies will have look-up access only.
Chartfields Agency Specific	PeopleTools Application	Decentralized	Configuration	PeopleTools Security and Application Security using SetID.	Appropriate agency users will have full access to these chartfiles but will be limited to the appropriate SetIDs.
Grants	Application	Decentralized	Configuration	Access controlled by Business Unit and SetID.	

Document Version Control

Version	Publication Date	Task Order	Description of Change	Author	Approver's Initials
1.0	Sept xx, 2003	xx	Initial Issuance		
2.0	Jan 22, 2004	01	Updated document to add information on centralized and de-centralized security	JK	
3.0	Feb 4, 2004		Updated recommendations	TKP	
4.0	Feb 24, 2004		Updated for deficiencies	TKP	
5.0	Feb 26, 2004		Updated Enterprise Tree administration	TKP	
6.0	Jun 03, 2004		Updated recommendations	AH	