1. **To: (Receiving Organization)**
2. Distribution
3. **From: (Originating Organization)**
4. Related EDT No.: N/A
5. Proj./Prog./Dept./Div.: HANDI 2000 INTEGRATION
7. Purchase Order No.: N/A
8. Originator Remarks:
9. Equip./Component No.: N/A
10. System/Bldg./Facility: N/A
11. Receiver Remarks:
12. Major Assy. Dwg. No.: N/A
13. Permit/Permit Application No.: N/A
14. Required Response Date: N/A
15. **DATA TRANSMITTED**

<table>
<thead>
<tr>
<th>(A) Item No.</th>
<th>(B) Document/Drawing No.</th>
<th>(C) Sheet No.</th>
<th>(D) Rev. No.</th>
<th>(E) Title or Description of Data Transmitted</th>
<th>Approval Designator</th>
<th>Reason for Transmittal</th>
<th>Originator Disposition</th>
<th>Receiver Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HNF-2713</td>
<td>N/A</td>
<td>REV 0</td>
<td>SECURITY ADMINISTRATION PLAN FOR HANDI 2000</td>
<td>N/A</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BUSINESS MANAGEMENTSYSTEM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16. **KEY**

- E, S, Q, D OR N/A
- (See WHC-CM-3-5, Sec. 12.7)

<table>
<thead>
<tr>
<th>Reason</th>
<th>Disp.</th>
<th>(J) Name</th>
<th>(K) Signature</th>
<th>(L) Date</th>
<th>(M) MSIN</th>
<th>(G) Reason</th>
<th>Disp.</th>
<th>(J) Name</th>
<th>(K) Signature</th>
<th>(L) Date</th>
<th>(M) MSIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Design Authority</td>
<td>DAWN E. ADAMS</td>
<td>G1-21</td>
<td>3</td>
<td>DIANE WILSON</td>
<td>G1-21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Design Agent</td>
<td></td>
<td></td>
<td></td>
<td>DOE/RL Reading Room</td>
<td>H2-53</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Cog. Mgr.</td>
<td></td>
<td></td>
<td></td>
<td>Central Files</td>
<td>B1-07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>QA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>Env.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

19. **SIGNATURE/DISTRIBUTION**

- (See Approval Designator for required signatures)

20. Design Authority/Cognizant Manager

21. DOE APPROVAL (if required)

- контрол №.

- Approved
- Approved w/comments
- Disapproved w/comments

**BD-7400-172-2 (10/97)**
SECURITY ADMINISTRATION PLAN FOR HANDI 2000 BUSINESS MANAGEMENT SYSTEM

Dawn E. Adams, FDH
2355 Stevens MSN G1-21
Richland, WA 99352
U.S. Department of Energy Contract DE-AC06-96RL13200

EDT/ECN: 625368 Org Code: SL610000 Charge Code: HANF6800
B&R Code: EW7001000 Total Pages: 24.7

Key Words: HANDI 2000, BUSINESS MANAGEMENT, SECURITY ADMINISTRATION, H2K, BMS, PEOPLESOFT, PASSPORT, TOOLS & METHODS, FINANCE, SUPPLY, CHEMICAL, HUMAN RESOURCES, PAYROLL, COTS

Abstract: This document encompasses and standardizes the integrated approach for security within the PP and PS applications. It also identifies the security tools and methods to be used. The Security Administration Plan becomes effective as of this document's acceptance and will provide guidance through implementation efforts and, as a "living document" will support the operations and maintenance of the system.

TRADEMARK DISCLAIMER. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors.

Printed in the United States of America. To obtain copies of this document, contact: Document Control Services, P.O. Box 950, Mailstop H6-08, Richland WA 99352, Phone (509) 372-2420; Fax (509) 376-4989.

PassPort (PP) is a trademark of Indus Corporation.
PeopleSoft (PS) is a trademark of PeopleSoft Corporation.
UNIX is a trademark licensed exclusively through X/Open Co. Ltd.
Oracle is a trademark of Oracle Corporation.
SQL is a trademark of Microsoft Corporation.

Approved For Public Release
SECURITY ADMINISTRATION PLAN

FOR

HANDI 2000

BUSINESS MANAGEMENT SYSTEM

Prepared by: Amanda McKay, LMSI Software Engineer

Prepared for: Fluor Daniel Hanford

Approved by:

Robert E. Gates, H2K Project Director

Steve Manley, FDH/CIO Manager

Dawn E. Adams, BMG Project Manager

Kristina Whiteaker, INDUS Project Manager

Phillip B. (Brian) Isaacs, LMSI Project Manager

James T. Stowe, Site Security Operations

Date
# TABLE OF CONTENTS

1 INTRODUCTION ........................................................................................................................................ 3  
1.1 OVERVIEW .................................................................................................................................. 3  
1.2 PURPOSE ...................................................................................................................................... 3  
1.3 SCOPE ........................................................................................................................................... 3  
1.4 ACRONYM DEFINITIONS ............................................................................................................. 4  
1.5 ROLES AND RESPONSIBILITIES ................................................................................................. 5  
1.6 REFERENCES ............................................................................................................................... 5  

2 NETWORK SECURITY .................................................................................................................................. 6  
2.1 UNIX ACCOUNT MANAGEMENT PROCESS ............................................................................ 6  
2.2 FILE ACCESS ................................................................................................................................ 7  
2.3 EXTERNAL SYSTEM INTERFACES ............................................................................................. 8  
2.4 FILE AND DATABASE SERVERS ................................................................................................. 8  
2.5 WORKSTATION SECURITY ......................................................................................................... 8  

3 PASSPORT ORACLE DATABASE SECURITY .......................................................................................... 9  
3.1 PASSPORT DATABASE CONSIDERATIONS ................................................................................ 9  

4 PEOPLESOFT RDMS DATABASE SECURITY ...................................................................................... 11  
4.1 PEOPLESOFT DATABASE CONSIDERATIONS ............................................................................ 12  

5 PASSPORT APPLICATION SECURITY .................................................................................................. 13  
5.1 PASSPORT APPLICATION CONSIDERATIONS .......................................................................... 13  

6 PEOPLESOFT APPLICATION SECURITY .......................................................................................... 15  
6.1 SECURITY PROFILES .................................................................................................................. 15  
6.2 OBJECT SECURITY ....................................................................................................................... 16  
6.3 ROW LEVEL SECURITY ................................................................................................................ 16  
6.4 QUERY SECURITY ......................................................................................................................... 17  
6.5 FIELD LEVEL SECURITY ............................................................................................................. 17  
6.6 FIELD AND RECORD AUDIT TRAIL ......................................................................................... 17  

7 APPENDIX A USER ACCESS FORM .................................................................................................. 18  

8 APPENDIX B PASSPORT SECURITY PROFILES ............................................................................... 23  

9 APPENDIX C PEOPLESOFT HR/PAYROLL/TRAINING SECURITY PROFILES .......................... 42
1 INTRODUCTION
1.1 OVERVIEW

The Hanford Data Integration 2000 (HANDI 2000) Project will result in an integrated and comprehensive set of functional applications containing core information necessary to support the Project Hanford Management Contract (PHMC). It is based on the Commercial-Off-The-Shelf (COTS) product solution with commercially proven business processes. The COTS product solution set, of Passport (PP) and PeopleSoft (PS) software, supports finance, supply, chemical management, human resources, and payroll activities under the current PHMC direction. The PP software is an integrated application for Accounts Payable, Contract Management, Inventory Management, Purchasing and Material Safety Data Sheets (MSDS). The PS software is an integrated application for Projects, General Ledger, Human Resources/Training, Payroll, and Base Benefits. This set of software constitutes the Business Management System (BMS) and MSDS, a subset of the HANDI 2000 suite of systems. To be referred to throughout this document as BMS.

This document provides a framework for communicating how security will be implemented and maintained across the Fluor Daniel Hanford, Incorporated (FDH) integrated components of the financial, supply, chemical management, human resource, and payroll modules. The primary objective is to minimize significant risks to the new System while ensuring access is reasonable and commensurate with job position functionality.

1.2 PURPOSE

This document encompasses and standardizes the integrated approach for security within the PP and PS applications. It also identifies the security tools and methods to be used. The Security Administration Plan becomes effective as of this document’s acceptance and will provide guidance through implementation efforts and, as a "living document", will support the operations and maintenance of the system.

1.3 SCOPE

The scope of security applies to the BMS applications. The system is comprised of the following vendor product modules as databases:

<table>
<thead>
<tr>
<th>Business Management System</th>
<th>Vendor Product</th>
<th>Vendor Modules</th>
<th>Operating System</th>
<th>DBMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance Management</td>
<td>PeopleSoft</td>
<td>General Ledger Projects Module</td>
<td>UNIX</td>
<td>Oracle</td>
</tr>
<tr>
<td>Supply Management</td>
<td>PassPort</td>
<td>Accounts Payable Inventory Management Contracts Management Purchasing</td>
<td>UNIX</td>
<td>Oracle</td>
</tr>
<tr>
<td>Chemical Management</td>
<td>PassPort</td>
<td>MSDS</td>
<td>UNIX</td>
<td>Oracle</td>
</tr>
<tr>
<td>Human Resources</td>
<td>PeopleSoft</td>
<td>Human Resources Training</td>
<td>NT</td>
<td>SQL Server</td>
</tr>
<tr>
<td>Payroll</td>
<td>PeopleSoft</td>
<td>Payroll Base Benefits</td>
<td>NT</td>
<td>SQL Server</td>
</tr>
</tbody>
</table>
This plan will consider three levels of security requirements: the network, application layer, and the Database Management Systems (DBMS).

This plan does not encompass security of data that has been extracted or exported from the BMS environment. Lockheed Martin Services, Incorporated (LMSI) will not be responsible for security or validity of that data, however, LMSI will assist FDH in identification and/or control mechanisms for this data.

1.4 ACRONYM DEFINITIONS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMS</td>
<td>Business Management System</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off The Shelf</td>
</tr>
<tr>
<td>DBA</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System - For BMS applications as follows: Oracle (for Passport Supply &amp; PeopleSoft Financials), SQL Server (for PeopleSoft Human Resources and Payroll)</td>
</tr>
<tr>
<td>DDL</td>
<td>Data Definition Language</td>
</tr>
<tr>
<td>DML</td>
<td>Data Manipulation Language</td>
</tr>
<tr>
<td>FDH</td>
<td>Fluor Daniel Hanford, Incorporated</td>
</tr>
<tr>
<td>H2K</td>
<td>HANDI 2000</td>
</tr>
<tr>
<td>HANDI 2000</td>
<td>Hanford Data Integration Project</td>
</tr>
<tr>
<td>HID</td>
<td>Hanford Identification [number]</td>
</tr>
<tr>
<td>HLAN</td>
<td>Hanford Local Area Network</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LMSI</td>
<td>Lockheed Martin Services, Incorporated</td>
</tr>
<tr>
<td>MSDS</td>
<td>Material Safety Data Sheets</td>
</tr>
<tr>
<td>OPS</td>
<td>LMSI Operations</td>
</tr>
<tr>
<td>PHMC</td>
<td>Project Hanford Management Contract</td>
</tr>
<tr>
<td>PP</td>
<td>Indus Passport software</td>
</tr>
<tr>
<td>PS</td>
<td>PeopleSoft software</td>
</tr>
<tr>
<td>SD&amp;I</td>
<td>Software Development &amp; Integration</td>
</tr>
</tbody>
</table>
1.5 ROLES AND RESPONSIBILITIES

Within each level, the defined scope will have specific responsibilities for security implementation and maintenance.

Roles and responsibilities in the area of security will be defined for two distinct phases for the BMS system (to be referred to as "the system" from this point forward):

- Identification and implementation of security and controls in a project implementation environment;
- Maintenance and regular review of security and controls in a production environment.

<table>
<thead>
<tr>
<th>Level of Security</th>
<th>Implementation Responsible Organization &amp; Position</th>
<th>Production Responsible Organization &amp; Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>LMSI/OPS Network Administrator</td>
<td>LMSI/OPS Network Administrator</td>
</tr>
<tr>
<td>UNIX Server Access</td>
<td>LMSI/OPS Password Administrator</td>
<td>LMSI/OPS Password Administrator</td>
</tr>
<tr>
<td>NT Server Access</td>
<td>LMSI/TEL Password Administrator</td>
<td>LMSI/TEL Password Administrator</td>
</tr>
<tr>
<td>PP Oracle Database</td>
<td>LMSI/OPS DBA</td>
<td>LMSI/OPS DBA</td>
</tr>
<tr>
<td>PS Oracle Database</td>
<td>LMSI/OPS DBA</td>
<td>LMSI/OPS DBA</td>
</tr>
<tr>
<td>PS SQL Database</td>
<td>LMSI/SDI DBA</td>
<td>LMSI/SDI DBA</td>
</tr>
<tr>
<td>PP Supply Application (Functional)</td>
<td>FDH System Administrator</td>
<td>FDH System Administrator</td>
</tr>
<tr>
<td>PP Supply Application (Technical)</td>
<td>LMSI/SDI Software Engineer</td>
<td>LMSI/SDI Software Engineer</td>
</tr>
<tr>
<td>PS Financial Application (Functional)</td>
<td>FDH System Administrator</td>
<td>FDH System Administrator</td>
</tr>
<tr>
<td>PS Financial Application (Technical)</td>
<td>LMSI/SDI Software Engineer</td>
<td>LMSI/SDI Software Engineer</td>
</tr>
<tr>
<td>PS HR/PR Application Technical</td>
<td>LMSI/SDI Software Engineer</td>
<td>LMSI/SDI Software Engineer</td>
</tr>
<tr>
<td>PS HR/PR Application Functional</td>
<td>FDH System Administrator</td>
<td>FDH System Administrator</td>
</tr>
</tbody>
</table>

1.6 REFERENCES

- HNF-2584 Region and Database Management Plan
- HNF-2858 Backup and Recovery for HANDI 2000 Software
- HNF-2859 Disaster Recovery for HANDI 2000 Hardware and Software
- HNF-PRO-592 Unclassified Computer Security Management Control Process
- HNF-2857 System Design Description
- Appendix A Security Access Form
- Appendix B Passport Security Profiles
- Appendix C PeopleSoft Security Profiles
2 NETWORK SECURITY

The network is comprised of the following components:

- Communication lines across the Wide Area Network (WAN) and Local Area Network (LAN)
- Fileservers
- Database servers
- User workstations

Network and database security controls will comply with existing FDH policies and guidelines. The departments and responsible hardware owners will administer network security and audit on file servers, workstations, and printers. Responsible LMSI organizations will ensure that policies are implemented in their appropriate areas.

Network Logon is the highest level of security for the system. Each Project Hanford Management Contract (PHMC) network user is assigned a user identification value, commonly referred to as Hanford Identification (HID) and password for authorized access to the network. Network operational procedures dictate enforcement of password changes on a regular basis and prevention of multiple unsuccessful logon attempts. These procedures will be applicable to BMS.

2.1 UNIX ACCOUNT MANAGEMENT PROCESS

A Password Administrator (PA) will set up a user account on the UNIX HANDI 2000 computer system. The security controls in place protect the system from unauthorized access, assure data integrity, and prevent misuse. Reference, HNF-PRO-592, Unclassified Computer Security Management Control Process, Section 5.0 guidelines. This security is necessary in order to gain entry to the Peoplesoft and Passport applications.

2.1.1 Password Access Controls

The password automatically expires every 90 days. The expiration date initializes when the new user logs on the system for the first time. Passwords shall be from six to eight characters in length, with at least one non-alphabetic. The password’s first character must be an alpha. There are controls established to prevent users from resetting passwords to a previous password.

User account passwords automatically expire every 90 days prompting the user to enter a new password. There are no restrictions regarding how often a password can be changed. Each time a password is changed it is encrypted to insure security.

To alert the System Administrator to possible intruder activity, a system log entry is made after five unsuccessful password entry attempts. There are scripts that generate an electronic mail message to the UNIX System Administrator that invalid attempts have taken place. The System Administrator reviews the log daily.

2.1.2 New Accounts

Either the Functional System Administrator or Data Owner will send an access request form to Technical Operations for a new user account to be set up on a particular system. The PA will perform the following:

- Assign the user a Unique User Identification (UID) enabling them to access all UNIX systems for which they are approved.
Assign the user an unique logon identification. This is typically the Hanford Identification (HID) number prefaced by an alphabetic character.

After the account and directory for new users are set up, a default password is assigned. The access request application will be returned to the Access Authorizer for notification that the account has been created. The application security can then be established.

The Access Authorizer will notify the new user of the logon identification and default password and coordinate any needed training.

The PA will send the new user, via electronic mail, a Password Verification form instructing the user on the proper use of passwords. The user will forward this message back to the PA, which indicates the user has read and understands the password rules. The forwarded form and the access request form will be retained by the PA for as long as the user has access to the system. If the user does not return this form within ten working days the account is suspended and a second request is sent. If no response from the user is received within five working days, the account is deleted from the system.

2.1.3 Delete Account

When the Access Authorizer notifies the PA of a user termination or transfer to another on-site company, the PA will immediately suspend the user account. The account will be deleted from the UNIX system within two days of notification. The PA will use a script to delete the logon id and directories from the password account file. The PA notifies the Access Authorizer of the UNIX system of terminated users that were deleted.

2.1.4 Change Password

The PA will make requested changes to user password files upon request; the most common request by users is to correct forgotten passwords. The PA will change the password to a default password and send the user an electronic mail message with the receipt of request and the new password. The system will prompt the user to enter a new password the next time the user logs on. This password will be encrypted to insure security.

2.1.5 Data Owner Account Review

On a quarterly basis, an updated list of all users is sent to the data owner's Access Authorizer for review along with a second list indicating "LAST LOGON" by users. This list indicates the last date the user logged onto the system. The Access Authorizer will send a request to the PA of any users no longer requiring access and will request the "LOGON ID" be deleted from the password account.

2.1.6 LMSI Account Review

The PA creates a list of all users including the last date the user logged onto the system. Users that have not logged on for 90 days or longer or have a status of "NEVER LOGGED ON" will be deleted from the system. The PA will notify the Access Authorizer of account deletions.

2.2 FILE ACCESS

The BMS executable files will reside on secured file servers. LMSI will list all directories and recommend read-only access to the directories where necessary.
2.3 EXTERNAL SYSTEM INTERFACES

When data is sent to systems external to BMS, the security and audit for that data becomes the responsibility of the recipient; LMSI will outline the security and audit considerations for that data. Once data has been extracted for use outside of the BMS systems (through a report, query, or interface), the security and audit for the data is no longer auditable by LMSI or BMS.

2.4 FILE AND DATABASE SERVERS

Physical access to fileservers will be restricted. Each server will also be password protected and have appropriate backup procedures based upon the maximum level of security required by any one segment of the integrated data. Reference HNF-2858, Backup and Recovery for HANDI 2000 Software and HNF-2859, Disaster Recovery for HANDI 2000 Hardware and Software.

NOTE: The Human Resources (HR) system contains training data. When users access the Training Matrix System (TMX) via the Hanford Local Area Network (HLAN) Intranet, they will be able to access specific training information within the HR system. User level security will be managed by a 'secure' Structured Query Language (SQL) connection which will permit only approved access to HR training data.

2.5 WORKSTATION SECURITY

Whenever a report is generated from within the system, the default output for the file is the C:TEMP directory. In this case, the data is no longer secure and becomes the responsibility of the person initiating the report. Each BMS user has the responsibility to abide by the FDH Computer Security Rules for closing down a "session" while away from the workstation.
3 PASSPORT ORACLE DATABASE SECURITY

The environment will consist of eight Oracle database instances (regions):
- Production Region
- Acceptance Region
- Development Region
- Practice Region
- Training Region
- DataLoad Region (Temporary)
- Demo Region
- Integration Region (Temporary)

The user roles requiring differing degrees of access rights to data in these database instances are:

**Network Administrator** -
- Processes requests by users for access to the HLAN
- Sets up LAN user accounts with an initial password.

**Server Administrator** –
- Sets up UNIX password accounts to allow logon/access to Database Servers.

**Functional System Administrator** –
- Business function
- application administration
- manages user approvals
- access, table values
- security profiles.

**Technical System Administration** –
- Technical function which manages the technical aspects of the systems,
- Implements user access, table values and security profiles

**Power Users** –
- Personnel utilizing PP to accomplish their daily work

**Periodic Users** –
- Personnel who may require the PP applications to do some of their work but not necessarily on a daily basis.
- **Casual Users** - Personnel who may require PP applications on an occasional basis.

NOTE: For additional information, Reference HNF-2884, Region and Database Management Plan and HNF-2857 System Design Document.

3.1 PASSPORT DATABASE CONSIDERATIONS

**Database Logon**

Direct access to the database operating environment will be given only to individuals with the proper approval. All other users will access the database strictly through the application. Data Definition Language (DDL) privileges will be restricted to the Database Administrator (DBA). Developers may still have Data Manipulation Language (DML) privileges, but will need the DBA to make physical changes to
the database structure. Reference Appendix A, User Access Form.

Query tools

Access to SQL*Plus, PS/Query, Crystal Reports and any other third party report writers will be used to perform queries. Access to these query and reporting tools will only be given to end-users once the system has stabilized, adequate training has been given and access need identified and approved.
4  PEOPLESOF T RDMS DATABASE SECURITY

PS Finance consists of seven databases:

- Production
- Acceptance
- Development
- Demo
- Practice
- Training
- Audit

PS Human Resources/Payroll consists of five databases:

- Production
- Development
- Demo
- Test
- Upgrade

For additional information, refer to HNF-2884, Region and Database Management Plan.

The following defines development, maintenance and user roles –

**Network Administrator**
- Processes requests by users for access to the HLAN
- Sets up LAN user accounts with an initial password.

**Server Administrator**
- Sets up UNIX password accounts to allow logon/access to Database Servers.

**Functional System Administrator**
- Business function
- application administration
- manages user approvals
- access, table values
- security profiles.

**Technical System Administration**
- Technical function which manages the technical aspects of the systems,
- Implements user access, table values and security profiles

**Power Users**
- Personnel utilizing PP to accomplish their daily work

**Periodic Users**
- Personnel who may require the PP applications to do some of their work but not necessarily on a daily basis.

**Casual Users** - Personnel who may require PP applications on an occasional basis.
The PS Tools application provides the ability to update data and to use a limited subset of the PeopleTools application. Tool access and capabilities will be implemented via the user class to which each HID user is associated. The options that are being considered for user class utilization are Nvision, Tree Manager, Process Scheduler, Process Monitor, and Query.

4.1 PEOPLESOF T DATABASE CONSIDERATIONS

Database Logon

Direct access to the database operating environment will be given only to individuals with the proper approval. All other users will access the database strictly through the application. DDL privileges will be restricted to the DBA. Developers may still have DML privileges, but will need the DBA to make physical changes to the database structure.

Query Tools

SQL*Plus, ISQL, PS/Query, Crystal Reports and any other third party report writers will be used to perform queries. Access to these query and reporting tools will only be given to end-users once the system has stabilized, adequate training has been given and access need has been identified and approved.
5 PASSPORT APPLICATION SECURITY

The final layer of PP security is implemented within the application itself. PP provides several alternatives for defining the degree of granularity necessary. The appropriate FDH business owners will determine the level of security required for their data. PP facilitates implementation of security with the following options:

- Security Events
- Security Event Type
  - Panel
  - Options
  - Execute Function
  - Generic Search
  - Rules Based (Field level security)
  - Program Defined
  - Simple Code
  - Custom
- Authorization Levels
- Primary Level Security
- Level Type
- Security Group
- Security Profile

5.1 PASSPORT APPLICATION CONSIDERATIONS

Security Events

The foundation of PP's security system is the Security Event. A Security Event is an identifier associated with the security checkpoints performed by the architecture, and in some cases application programs. The Security Event tells what authorization should be used at the security checkpoint.

Security Event Type

Security Event Types categorize Security Events with types such as panel, option, and execute.
- Panels have Security Events associated with them to allow the client to provide update, read, or no access to each panel.
- Options are menu options and may have security events controlling who has discrete option privileges on panel menus.
- The Execute Function controls access to the action associated with the Execute Command.

Authorization Levels

Authorization levels are the different levels of activity which a user may be authorized to perform on a Security Event:
- Update
- Read-only
- None
Authorization levels are assigned to Security Events only within a Security Profile.
Primary Level Security

Primary Level Security refers to data, which has a relationship to a global data element. This element is determined at system generation time and is typically Facility. If the value of Facility on the panel matches the default Facility for the user, then that is the user’s own data. If the two values do NOT match, then the user is looking at other data. This may allow different access authorizations to be specified when a user's own Facility matches the facility associated with the data and when a user's own Facility does not match the data Facility.

Level Type

Level Type Security type determines what type of security authorizations and checking will be performed for a particular Security Event at the primary levels.

- **Own/Other** - grant and check for different authorization levels depending upon whether the data is the user's "own".
- **Unconditional** - allows authorization to be granted and checked with independence of the element and data associated with the Primary Level security.
- **None** - This level is not being used with this application.

Security Groups

After Security Events, Security Groups are the next level of security. Security Groups are a logical combination of security events. A group is typically composed of related events to which a specific set of users would need the same access. The same authority will be granted later to a user or specified set of users to all the events in requested group.

Security Profiles

A Security Profile consists of a logical combination of Security Groups and/or Security Events, usually tailored to a group of users who have the same system access needs. A user can be assigned a single Security Profile, multiple Security Profiles or a combination of Security Profiles and Security Events. Typically a Security Profile is defined and assigned to a large group of users needing the same authorization levels to the same PP panels. The FDH Project Leads for Supply, Human Resources, and Payroll will finalize Security Profiles by approving the profiles. Approval will be denoted by their signatures.

User Profile

A User Profile consists of a logical combination of Security Profiles and/or Security Events which provide a user with secured system access that meets their particular job requirements. A User Profile may consist of several Security Profiles or Security Events or just one Security Profile or Security Event. If a user is associated with multiple profiles, the maximum "rights" are utilized. Each user will have their own User ID (equivalent to the UNIX user account). The Functional Administrator will assign the appropriate security profiles to individuals. FDH will ensure that appropriate training accompanies the assignment of a Security Profile to a user. For detailed information on PeopleSoft Human Resources/Payroll Operator Class Security Specifications Reference HNF – 2857 System Design Description.
6 PEOPLESOFT APPLICATION SECURITY

The final layer of PS security is implemented within the application itself. The PS application offers multiple tools and options for security. It may not be necessary to utilize all aspects of PS security. PS facilitates implementation of security with the following options:

- Operator and Operator Class Security (Security Profiles)
- Security Trees
- Object Security
- Row Level Security by:
  - Project
  - Analysis Group
  - Ledger
- Query Security
- Field Level Security
- Field and Record Audit Trail

The following section provides details on the PS security tools. For additional application level security information, reference Appendix B for Finance and Appendix C for Human Resources and Payroll.

6.1 SECURITY PROFILES

The Technical System Administrator will maintain control of the non-production (i.e. Development and Acceptance) database regions and will assign access on an as needed basis. Functional security profiles will be utilized in the production environment.

Security Profiles

Security profiles are defined using PS Security Administrator. Each Operator Class (security profile) is defined according to the business processes that it requires access to. An individual may require a new Operator Class in order to meet a specific need, however, the decision to implement the new class will be made after proper change control approvals. Each user will require his or her own ID. The Security Administrator (Functional Administrator) will assign individuals to the appropriate Operator Classes, however, the business owner will determine which Operator Class a user will be assigned. FDH will ensure appropriate training accompanies the assignment of a security profile to a user. For detailed information on PeopleSoft BMS Financials Operator Class Security Specifications and PeopleSoft BMS HR/PR Operator Class Security Specifications Reference HNF – 2857 System Design Description

Panel Security

Panel access will be granted to users when it is needed for completing one’s job assignments. This approach will provide users with only those areas that they need access to in order to fulfill the business need and reduce "menu clutter". However, all modules and panels will be accessible in a test environment.

Corrective Action

Correcting historical data is accomplished with Corrective Action. Use of the Correction action will be severely limited. Only specific users will be given full access to the Correction action in PS. This is to ensure that historical records are not updated without an adequate audit trail, and that the integrity of the data is maintained. Department users will only be given access to Correction where the business process
demands it and only after appropriate training has been received.

6.2 OBJECT SECURITY

Through Object Security, PS offers the capability to secure access to the various objects within the application. The specific objects that can be secured include import definitions, menu definitions, panel group definitions, panel definitions, query definitions, record definitions, tree definitions, and projects. In a development environment it may be desirable to limit access to some of these objects. For example, once key panels and menus have been configured for production it may be necessary to restrict who has edit capabilities over these objects. It is also possible to create object groups that represent a specific area such as the general ledger. In this manner, access can be assigned only to object groups within a user's domain.

PS also offers the ability to restrict access to an entire object type - records, panels, etc. - using the Application Designer. This serves to control access to the Application Designer functionality that handles a particular type of object.

It should be noted that it is not always necessary to employ object level security, this is especially true when the size of the project team is relatively small and the group is knowledgeable. It is not needed if all developers require access to all application definitions. Currently, Finance does not plan to use Object Security.

6.3 ROW LEVEL SECURITY

PS offers the capability to secure access to specific rows of data within the database based on a number of attributes: Analysis Group, Ledger, Projects, Set ID, or Business Unit. Only one Business Unit and Set ID is being implemented and therefore, unlikely there will be a need to implement any row-level-security for these areas. However with Ledgers, Projects or Analysis Groups there may be requirements for row-level security.

Projects

Security for the project field is based on Project Trees. Within project security, the Tree Manager can control which users have access to each project through the Tree Manager. For example, project security can limit access to only one distinct project that a particular analyst or manager supports. The requirements for project level security will not be determined until the final list of system operator profiles is complete and the business need has be defined for restricting access to information. It is also necessary to wait for the list of valid Project ID's to avoid having to duplicate efforts. Currently, Finance does not plan to use Project level security. If Project level security were to be utilized, it will be necessary to build Project Trees in the system prior to assigning trees to operator classes.
Ledgers

Ledger Security limits access to specific Ledger Types, Ledger Groups or individual ledgers. For example, there may be a requirement to allow users access to budget ledgers without allowing them access to the actuals ledger. It is also possible to secure access to specific nVision ledgers or business units, which will ensure that users can't create nVision reports that cut across ledgers to which they shouldn't have access.

6.4 QUERY SECURITY

Query takes advantage of operator profiles and row level security to allow how to control what query operations a user can perform and what data they can access using Query. Query options or functions are controlled for users via their Query Profile. For example, users may be able to run existing queries but not allowed to create new ones. Query types may be limited as well as the output options (i.e. Excel, Crystal).

PS also uses Access Groups to provide a logical organization to records for user access. For example, an accounting user may have access to the General Ledger Access Group (which contains all the related records for that function). Access Groups are nodes in a query tree which are built with Tree Manager. Once a query tree has been built, users may be granted access to one or more of its Access Groups. The user can then generate queries on any tables in the Access Groups accessible to them.

Once system users and their information requirements are identified, specific levels of access and appropriate Query access will be assigned. Access Groups will be utilized as much as possible. New Access Group will be added to meet specific requirements for additional tables.

6.5 FIELD LEVEL SECURITY

PeopleCode can restrict access to particular fields or columns within application tables. For example, if a certain class of operator needs to be able to access certain panels, but not to view a particular field on those panels, PeopleCode can hide the field for that operator class. At this point, PS recommends this functionality not be implemented because it entails customization of the application and would have upgrades implications.

6.6 FIELD AND RECORD AUDIT TRAIL

Through Field and Record audit trail, PS provides the ability to maintain a full audit trail at either the field or record level. This will be provided only for those processes requiring an audit trail due to impact to on-line performance and required disk space. LMSI will be responsible for providing adequate reports and/or tools for audits where an audit has been deemed necessary.
## Appendix A User Access Form

**REQUEST FOR USER APPLICATION ACCESS**

**DATE:**

**IMPORTANT NOTICE:** Workstation required configuration for system access must be: **CASUAL USERS** a minimum 486/33 with 16 mg RAM and Windows 95 installed. **ALL OTHERS** a minimum Pentium 100 with 32 mg RAM and Windows 95 installed. Install through Software Distribution.

**INSTRUCTIONS (Print or Type)**
- Please complete all applicable information about the person requiring access.
- Return completed forms to Security Administration G1-57.

<table>
<thead>
<tr>
<th>User Name (last, first, mi)</th>
<th>Hanford ID</th>
<th>Company</th>
<th>Cost Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td>CPU Number</td>
<td>Work Location (bldg./area/room)</td>
<td>Work Phone Number</td>
</tr>
<tr>
<td>Manager Name (last, first, mi)</td>
<td>Hanford ID</td>
<td>Work Phone No.</td>
<td>Manager Signature</td>
</tr>
</tbody>
</table>

Select User Access Additions/Changes; all selected user access privileges MUST be supported by the Kind of Function or Information Access Required narrative.

<table>
<thead>
<tr>
<th>TYPE OF USER ACCESS REQUEST:</th>
<th>PASSPORT USERS:</th>
<th>Annual Access Review Only. Access must be (check one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ New</td>
<td>Default Printer Address:</td>
<td>□ Maintained</td>
</tr>
<tr>
<td>□ Change</td>
<td>□ Local</td>
<td>□ Upgraded</td>
</tr>
<tr>
<td>□ Inactivate User Access</td>
<td>□ Network</td>
<td>□ Downgraded</td>
</tr>
<tr>
<td></td>
<td>Network Printer Address:</td>
<td>□ Deleted (no longer required)</td>
</tr>
</tbody>
</table>

**Kind of Function or Information Access Required:**

<table>
<thead>
<tr>
<th>Business Process Owner Approval:</th>
<th>System Administrator Approval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date: ________________________</td>
</tr>
<tr>
<td></td>
<td>Date: ________________________</td>
</tr>
</tbody>
</table>

***PassPort Users Only***

<table>
<thead>
<tr>
<th>Function</th>
<th>Approval level</th>
<th>Auto-Approve</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material request</td>
<td>level $</td>
<td>YES</td>
<td>Stock &amp; JIT orders (WIMS)</td>
</tr>
<tr>
<td>Material Requisition</td>
<td></td>
<td></td>
<td>Material purchases only</td>
</tr>
<tr>
<td>Contract Requisition</td>
<td></td>
<td></td>
<td>Contracts Only</td>
</tr>
<tr>
<td>Buyer</td>
<td></td>
<td></td>
<td>Purchase order and Amendment threshold</td>
</tr>
<tr>
<td>Buyer Manager</td>
<td></td>
<td></td>
<td>Purchase order and Amendment threshold</td>
</tr>
<tr>
<td>Contract Admin</td>
<td></td>
<td></td>
<td>Contracts and Amendment threshold</td>
</tr>
<tr>
<td>Contract Manager</td>
<td></td>
<td></td>
<td>Contracts and Amendment threshold</td>
</tr>
<tr>
<td>Contract Pay</td>
<td></td>
<td></td>
<td>Payments Authorization only</td>
</tr>
<tr>
<td>Authorize</td>
<td>Pending Status Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Add</td>
<td>System Admin function only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Update</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A/P Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A/P Invoice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A/P Vendor</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SECURITY PROFILES – FOR SECURITY ADMINISTRATION USE ONLY.**

- **PEOPLESOFT**
  - **FINANCE**
    - [ ] Technical System Administration
    - [ ] Functional Administration
    - [ ] Technical Support
    - [ ] Project Controls Group
    - [ ] Accounting Lead
    - [ ] GL Accountant
    - [ ] Treasury/AP Accountant
    - [ ] Cost Accountant
    - [ ] Funds Control Analyst
    - [ ] Project Budget Analyst
    - [ ] Other
    - [ ] Program Analyst

- **PEOPLESOFT**
  - **PAYROLL/HUMAN RESOURCES**
    - [ ] Technical System Administration
    - [ ] PeopleSoft Panels
    - [ ] Crystal Reports
    - [ ] PeopleSoft and Crystal

**PASSPORT**

**AP, PURCHASING, INVENTORY, CONTRACT MANAGEMENT, CHEMICAL MANAGEMENT**
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Access Privilege</th>
<th>Feature Description</th>
<th>Access Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical System Administration</td>
<td>Read Only</td>
<td>AP Invoice Auditor</td>
<td>Read Only</td>
</tr>
<tr>
<td>Office Support</td>
<td>Read Only</td>
<td>AP Payment Approver</td>
<td>Read Only</td>
</tr>
<tr>
<td>Material Requisitioners</td>
<td>Read Only</td>
<td>AP EDI</td>
<td>Read Only</td>
</tr>
<tr>
<td>Contract Requisitioners</td>
<td>Read Only</td>
<td>AP Checks</td>
<td>Read Only</td>
</tr>
<tr>
<td>Requisition Review/Approve</td>
<td>Read Only</td>
<td>AP Misc</td>
<td>Read Only</td>
</tr>
<tr>
<td>Buyers</td>
<td>Read Only</td>
<td>Vendor Administrator</td>
<td>Read Only</td>
</tr>
<tr>
<td>Buyer Manager Contract Administrator</td>
<td>Read Only</td>
<td>Vendor Input</td>
<td>Read Only</td>
</tr>
<tr>
<td>Contract Admin Manager</td>
<td>Read Only</td>
<td>Inventory Manager</td>
<td>Read Only</td>
</tr>
<tr>
<td>Buyer Tech Representative</td>
<td>Read Only</td>
<td>Warehouse Manager</td>
<td>Read Only</td>
</tr>
<tr>
<td>Inventory Management Specialist</td>
<td>Read Only</td>
<td>MSDS System</td>
<td>Read Only</td>
</tr>
<tr>
<td>Warehouse Store Keeper</td>
<td>Read Only</td>
<td>AP System Administrator</td>
<td>Read Only</td>
</tr>
<tr>
<td>QC Inspection Chemical Inventory Specialist</td>
<td>Read Only</td>
<td>Security System Administrator</td>
<td>Read Only</td>
</tr>
<tr>
<td>Master Catalog Administrator</td>
<td>Read Only</td>
<td>Finance Integration System Administrator</td>
<td>Read Only</td>
</tr>
<tr>
<td>Treasury</td>
<td>Read Only</td>
<td>Purchasing/CM System Administrator</td>
<td>Read Only</td>
</tr>
<tr>
<td>AP 1099</td>
<td>Read Only</td>
<td>Contract Amendments</td>
<td>Read Only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contract Payments</td>
<td></td>
</tr>
</tbody>
</table>

**DATABASE ADMINISTRATION (DA) OR SOFTWARE ENGINEER (SE) USE ONLY**

- **ASSIGNED DATABASE**
  - Practice
  - Training
  - Audit
  - Upgrade
  - Other

**Date Access Profile Completed:** ________________ **Date Password Assigned:** ________________

**Date Update Entered:** ________________ **Date Analyst Notified:** ________________

**DA or SE Signature:** ________________ **Date:** ________________

**Systems Analyst Signature:** ________________ **Date:** ________________
REQUEST FOR USER ACCESS FORM COMPLETION INSTRUCTIONS

1.0 PURPOSE

This form is used to document management authorization of PHMC personnel authorized to access the HANDI 2000 project modules.

2.0 SCOPE

This form must be prepared for any PHMC employee requesting access to the HANDI 2000 project modules.

3.0 RESPONSIBILITIES

The employees' manager shall ensure that a new access form is prepared and submitted to Security Administration when their employee requires:

- New access
- Changes to an existing security profile
- No longer requires access

The employees' manager shall also ensure that an exiting employee completes the User Access form to terminate access as part of the exit interview process.

4.0 PROCEDURE

4.1 Complete all the user information in Block 1.
4.2 Complete Type of User Access Request.
4.3 Annual Access Review Only. - Leave blank and System Administrator will complete.
4.4 Complete the Kind of Function or Information Access Required information in Block 3 - provide a description of how the employee will use the business functions to perform their job duties.
4.5 Business Process Owner Approval in Block 3 - leave blank and Business Process Owner will review and sign authorizing employee access.
4.6 System Administrator Approval in Block 3 - leave blank and System Administrator will review and sign authorizing employee access.
4.7 For Passport Users only: Approval level - completed by the authorizing manager and required if the employee will be allowed to automatically approve material requests or is a purchasing or contract administrator. Contract administrators should designate approval levels for contract requisitions, amendments, and payments.
4.8 For Passport Users only: Auto Approve Indicator - complete by placing a checkmark after the appropriate approval level category.
4.9 For Passport Users only: Approval Dollar Level - complete by identifying the maximum dollar level the employee is authorized to approve for materials requests, materials purchase orders (buyer signature authority level), contract requisitions (buyer signature authority level), contract amendment, and contract payment authority level.
4.10 Send the completed forms to Security Administration MSIN G1-57.
4.11 Completed forms received at Security Administration will be routed to the appropriate Security Administrator.
4.12 The functional Security Administrator will review the form for completeness and coordinate review and approval with the appropriate Business Process Owner.
4.13 Business Process Owner reviews and approves the form and returns the approved form to the functional Security Administrator for assignment of the database(s) and employee security access profile(s) that match the access information provided in step 3.9.
4.14 The completed form is submitted to the Data Base Administrator for setup of the user password. Passport users will also be assigned a UNIX account. The Security Administrator will assign the password and forward request to the UNIX account administrator (if appropriate).
4.15 If appropriate, the UNIX account administrator will assign an account to the employee and send the required UNIX account authorization form to the employee for completion.
4.16 The Security Administrator will notify the employee when their access is setup and ready for use.
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Office Support                    | Clerical and office administrative personnel responsible for entering orders basic cataloged office supplies in support of the line organization | • Master catalog  
• Material request  
• Vendor Search  
• Electronic approval routing  
• In-line order status  
• View MSDS  
• Purchase requisitions | GEN-001  
Course No. 085000  
PassPort General Supplies Workshop for Office Support and PHMC Employees | No | Systems Basics Portal/97 CBT | Shari Bultena (Inventory)  
Kim Schultz (Purchasing)  
Mike Stephenson (MSDS) | Auto -Approve Material Requests |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Material Requisitioner            | Project personnel responsible for ordering materials from on-site and off-site sources.         | - Master catalog  
- Material request  
- Vendor Search  
- Electronic approval routing  
- On-line order status  
- View MSDS  
- Purchase requisitions  
- Statement of Work  
- Std. Clauses  
- Contract Requisitions  
- Vendor Search  
- Multi-year milestones  
- Contract payment status  
- Contract amendments  
- Electronic approvals                                                                 | CON001/PUR001  
Note: Combined class.  
Course No. 085005  
PassPort Contract Administration and Purchasing for Requisitioners | No                                                   | Systems Basics Portal/97 CBT                                                | Shari Bultena (inventory)  
Kim Schultz (purchasing)  
Mike Stephenson (MSDS)  
Stan Cottrell (contract mgt.) | Auto-Approve Material Requests                                                              |
| Contract Requisitioner            | Project personnel responsible for preparing statements of work to request services from on-site and off-site sources. | - Electronic approvals  
- Material requests  
- Purchase requisitions  
- Contract requisitions                                                                 | CON001/PUR001  
Note: Combined class.  
Course No. 085005  
PassPort Contract | No                                                   | Systems Basics Portal/97 CBT                                                | Stan Cottrell (contract mgt.) | Auto-Approve Contract Requisitions                                                              |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Requisition Reviewers               | PHMC managers, who have signature authority to approve requisitions, authorize sole sources; review open workloads, and track cost expenditures. | • Purchase requisitions  
• Request for Proposals  
• Vendor Search  
• Award purchase order  
• Expedite P.O.  
• P.O. Revisions  
• Payment status  
• Purchasing analysis reports | CON002/PUR002  
Note: Combined Class.  
Course No. 085010  
PassPort Contract Administration and Purchasing Workshop for Approving and Reviewing Management | No | System Basics Portal/97 | Chris Hopkins (supply chain mgt.) | Yes | Dollar signature level |
| Buyers                              | Manages the work of Procurement personnel who prepare and issue purchase orders for material items. | • Open buyer requisition backlog  
• Purchase requisitions  
• Request for Proposals  
• Vendor Search  
• Award purchase order  
• Expedite  | PUR003  
Course No. 085020  
PassPort Purchasing Workshop for Buyers | Yes | Challenge course must complete System Basics Portal/97 CBT | Kim Schultz (purchasing) Shari Bultena (inventory mgt.) | Buyer procurement authority approval level required for purchase requisitions and P.O. revisions. |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer Manager</td>
<td>Procurement personnel who prepares and issues purchase orders for material items.</td>
<td>• Contract requisitions • Request for Quotes • Vendor Search • Award contract purchase order • Multi-year milestones • Contract amendments • Payment approvals • Payment</td>
<td>PUR003 Course No. 085020 Passport Purchasing Workshop for Buyers</td>
<td>Yes; Challenge Course by Demonstrating ability to navigate in Passport and perform buyer backlog review and assignment, and basic contract administration module functions.</td>
<td>Yes if challenging course must complete System Basics Portal/97 CBT</td>
<td>Kim Schultz (purchasing) Shari Bultena (inventory mgl.)</td>
<td>Buyer Manager procurement authority approval level required for purchase requisitions and P.O. revisions.</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>Passport Access/Functions</td>
<td>Passport Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
| Contract Administrator             | Procurement personnel who prepare and issue purchase orders for services. | status  
  - Contract analysis reports  
  - Assign open contract requisition buyer backlog  
  - Contract requisitions  
  - Request for Quotes  
  - Vendor Search  
  - Award contract purchase order  
  - Multi-year milestones  
  - Contract amendments  
  - Payment approvals  
  - Payment status  
  - Contract analysis reports | CON004  
  Course No. 085025  
  PassPort Contract Administration for Contract Administrators | Yes  
  Challenge Course by Demonstrating ability to navigate in PassPort and perform basic purchasing module functions. | Yes if challenging course must complete System Basics Portal/97 CBT | Kim Schultz (Contract mgt.) Bob Allen (Vendors) Brent Wagner (accounts payable) | Contract administrator procurement authority approval level required for contract requisitions contract amendments, and contract payments. |
| Contract Administrator Manager     | Manages the work of Procurement personnel who prepare, issue, and administer contract purchase orders | status  
  - Contract requisitions  
  - Statements of work  
  - Contract amendments  
  - Payment authorization | CON004  
  Course No. 085025  
  PassPort Contract Administration for Contract Administrators | Yes; Challenge Course by Demonstrating ability to navigate in PassPort and perform buyer backlog review | | | |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>Passport Access/Functions</th>
<th>Passport Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>for services.</td>
<td></td>
<td>s</td>
<td>Payment status</td>
<td>and assignment, and basic contract administration module functions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buyer Technical Representative</td>
<td>Project personnel who are responsible for reviewing and approving payment approvals for services performed on contracts.</td>
<td>Master catalog</td>
<td>Course No. 085035 PassPort Contract and Purchasing Workshop for Buyer Technical Reps.</td>
<td>No</td>
<td>System Basics Portal/97 CBT</td>
<td>Kim Schultz (contract mgt.) Brent Wagner (accounts payable)</td>
<td>No</td>
</tr>
<tr>
<td>Inventory Management Specialist</td>
<td>Project personnel who are responsible for maintaining adequate stocking levels for general supplies, spare parts; convenience storage, special tools, and equipment</td>
<td>Master catalog</td>
<td>INV-001 Course No. 085040 PassPort Inventory Mgt. for Inventory Mgt. Specialists.</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Shari Bultena (inventory mgt.) Kim Schultz (purchasing) Bob Allen (vendors)</td>
<td>Approve new Master Catalog ID's Cycle Count Variance Approval</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
| Warehouse Storekeeper             | Project personnel who are responsible for performing warehouse work associated with receiving, disbursing, counting, and shipping general supplies, spare parts, convenience storage, special tools, and equipment stocked in Materials Mgt. controlled warehouses. | - Master catalog  
- Material requests  
- Purchase requisitions  
- Purchase orders  
- Standards and procedures  
- Vendor search  
- Central receiving log  
- OSD&D  
- Electronic approvals | INV-002  
Course No. 085045  
PassPort Inventory Management for Warehouse Personnel | Yes | System Basics Portal/97 CBT | Shari Bultena (inventory mgt.)  
Kim Schultz (purchasing)  
Bob Allen (vendors) | Auto approve material requests |
| QC Inspection                     | Project personnel that are responsible for quality control receiving inspection for material items received at the 2355 Stevens central receiving warehouse. | - Master catalog  
- Material request  
- Facility transfers  
- Central receiving log  
- Warehouse locations  
- Material reservations  
- Vendor | INV-003  
Course No. 085050  
PassPort Inventory Mgt. for Quality Control Inspectors | Yes | System Basics Portal/97 CBT | Shari Bultena (inventory mgt.)  
Kim Schultz (purchasing)  
Bob Allen (vendors)  
Mike Taylor (standards and procedures) | No |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Chemical Inventory Specialist     | Project personnel responsible for the receipt, warehousing, disbursement, disposal, and physical inventorying of chemical inventories within Project facilities. | search:  
- OSD&D Warehouse distribution  
- Shipping  
- Cycle counting  
- Tier II reporting  
- MSDS  
- Schedule cycle counts  
- Master catalog  
- Material request  
- Central receiving log  
- Warehouse locations  
- Material reservations  
- Vendor search  
- OSD&D  
- QC inspection  
- Warehouse distribution  
- Shipping | INV-004  
Course No.  
085055  
PassPort Inventory Management for Chemical Inventory Mgt. Specialists | Yes | System Basics Portal/97 CBT | Mike Stephenson (Chemical inventory mgt. and MSDS)  
Shari Bultena (master catalog)  
Bob Allen (vendors)  
Kim Schultz (purchasing) | No |
| Warehouse Manager                 | Manager of Project personnel who are responsible for performing warehouse work associated with receiving, | Invoice search  
- Payment status  
- Print checks  
- Reconcile bank accounts | INV-002  
Course No.  
085045  
PassPort Inventory Management for Warehouse Personnel | Yes | System Basics Portal/97 CBT | Shari Bultena (inventory mgt.)  
Kim Schultz (purchasing)  
Bob Allen (vendors) | Auto Approve material requests |
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treasury</td>
<td>Accounting staff responsible for approving and printing checks for payments to satisfy outstanding accounts payable.</td>
<td>• On-demand payments&lt;br&gt;• Approve checks&lt;br&gt;• EFT transmission verifications&lt;br&gt;• Cash wires&lt;br&gt;• Check signing</td>
<td>AP-001 PassPort Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable)&lt;br&gt;Bob Allen (vendors)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>disbursing, counting, and shipping general supplies, spare parts, convenience storage, special tools, and equipment stocked in Materials Mgt. controlled warehouses.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>AP Invoice Auditor</td>
<td>Accounting personnel responsible for entering invoices, generating verifications of service for payment approvals, reconciling invoices and payments, and entering vendor remit to information.</td>
<td>processing</td>
<td>AP-001 PassPort Accounts Payable</td>
<td>Yes</td>
<td>System Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>No</td>
</tr>
<tr>
<td>AP Payment Approver</td>
<td>Accounting personnel responsible for approving payments for the purpose of authorizing payment of outstanding company payables.</td>
<td>Create new vendor Update vendor information Update vendor remit to information Vendor status</td>
<td>AP-001 PassPort Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>Yes (Dollar signature level)</td>
</tr>
<tr>
<td>AP Misc</td>
<td>Accounting personnel responsible for various AP tasks</td>
<td>Deleting invoices administering recurring invoices &amp; recurring payment schedules entering</td>
<td>PASSPORT Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>Yes (Dollar signature level)</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>AP EDI</td>
<td>Accounting personnel responsible for administering EDI freight bills</td>
<td>• cash receipts performing contract &amp; PO invoice overrides</td>
<td>PASSPORT Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>Yes Dollar signature level</td>
</tr>
<tr>
<td>AP Checks</td>
<td>Accounting personnel responsible for running check processing</td>
<td>• execute check batch for prelim payment register • process immediate payments • cancel checks</td>
<td>PASSPORT Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>Yes Dollar signature level</td>
</tr>
<tr>
<td>AP 1099</td>
<td>Accounting personnel responsible for administering 1099 reporting</td>
<td>• update 1099 info. • run 1099 reports • launch 1099 processings</td>
<td>PASSPORT Accounts Payable</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Brent Wagner (accounts payable) Kim Schultz (purchasing &amp; contract mgt.) Bob Allen (vendors)</td>
<td>No</td>
</tr>
<tr>
<td>Vendor Input</td>
<td>Purchasing and Accounts Payable personnel responsible for entering initial vendor</td>
<td>• enter vendors in Passport only</td>
<td>PUR003 Course No. 085020 PassPort Purchasing Workshop for Buyers</td>
<td>PUR-003 PassPort Purchasing Workshop for Buyers</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Kim Schultz (purchasing &amp; contract mgt.) Brent Wagner (accounts payable) Bob Allen</td>
<td>No</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Vendor Administrator</td>
<td>Purchasing and Accounts Payable personnel responsible for maintaining vendor information in PassPort.</td>
<td>• Master catalog&lt;br&gt; • Material request&lt;br&gt; • Electronic approvals&lt;br&gt; • Cycle counting&lt;br&gt; • Replenishments&lt;br&gt; • Standards and procedures&lt;br&gt; • Purchase requisitions&lt;br&gt; • Inventory mgt. analysis</td>
<td>PUR003&lt;br&gt; Course No. 085020&lt;br&gt; PassPort&lt;br&gt; Purchasing Workshop for Buyers</td>
<td>PUR-003&lt;br&gt; PassPort&lt;br&gt; Purchasing Workshop for Buyers</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Bob Allen (vendors)</td>
<td>No</td>
</tr>
<tr>
<td>Inventory Manager</td>
<td>Manager of the Project personnel who are responsible for maintaining adequate stocking levels for general supplies, spare parts, convenience storage, special tools, and equipment financial and non-financial controlled</td>
<td>• Proficient knowledge of the PassPort MSDS product&lt;br&gt; • Product specs.&lt;br&gt; • Documenting end user requirements&lt;br&gt; • Ad Hoc reporting&lt;br&gt; • Security setup and maint.&lt;br&gt; • MS Access&lt;br&gt; • Crystal</td>
<td>INV-001&lt;br&gt; Course No. 085040&lt;br&gt; PassPort&lt;br&gt; Inventory Mgt. for Inventory Mgt. Specialists.</td>
<td>Yes</td>
<td>Systems Basics Portal/97 CBT</td>
<td>Shari Bultena (inventory mgt.)&lt;br&gt; Kim Schultz (purchasing)&lt;br&gt; Bob Allen (vendors)</td>
<td>Approve new Master Catalog ID’s&lt;br&gt; Cycle Count&lt;br&gt; Variance&lt;br&gt; Approval</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>inventories.</td>
<td></td>
<td>Report Writer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Maint. of users guides</td>
<td></td>
<td>Business rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Monitor ABEND log</td>
<td></td>
<td>Routing lists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>MSDS System Administrator</td>
<td>Person responsible for managing, verifying, and maintaining the preferences, simple, and complex code tables for the PassPort MSDS module. Administrator is also responsible for reviewing and approving security access forms for user access to the PassPort MSDS module.</td>
<td>Proficient knowledge of the PassPort Accounts Payable, inventory mgmt., purchasing, contract mgmt., and financial integration products</td>
<td>PassPort System Administrator MSDS-001 PassPort MSDS</td>
<td>Yes</td>
<td>No</td>
<td>Tim Stokes (training coordinator) Mike Stephenson (MSDS)</td>
<td>No</td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>AP System Administrator</td>
<td>Person responsible for managing, verifying, and maintaining the preferences, simple, and complex code tables for the PassPort MSDS module. Administrator is also responsible for reviewing and approving security access forms for user access to the PassPort MSDS module.</td>
<td>rules • Monitor ABEND log • Routing lists</td>
<td>PassPort System Administrator AP-001 PassPort Accounts Payable</td>
<td>Yes</td>
<td>No</td>
<td>Tim Stokes (training coordinator) Brent Wagner (accounts payable)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Finance Integration System Administrator</td>
<td>Person responsible for managing, verifying, and maintaining the preferences, simple, and complex code tables for the PassPort MSDS module. Administrator is also responsible for reviewing and approving security access forms for user access to the PassPort MSDS module.</td>
<td>• Security setup and maint. • MS Access • Crystal Report Writer • Maint. of users guides • Business rules • Monitor ABEND log • Routing lists</td>
<td>PassPort System Administrator AP-001 PassPort Accounts Payable</td>
<td>Yes</td>
<td>No</td>
<td>Tim Stokes (training coordinator) Terry Main (financial integration)</td>
<td>No</td>
</tr>
</tbody>
</table>

Person responsible for managing, verifying, and maintaining the preferences, simple, and complex code tables for the PassPort MSDS module. Administrator is also responsible for reviewing and approving security access forms for user access to the PassPort MSDS module.
<table>
<thead>
<tr>
<th>User Role/PassPort Security Profile</th>
<th>User Responsibility Description</th>
<th>PassPort Access/Functions</th>
<th>PassPort Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchasing and Contract Mgt. System Administrator</td>
<td>Person responsible for managing, verifying, and maintaining the preferences, simple, and complex code tables for the PassPort Purchasing and Contract Mgt. Modules. Administrator is also responsible</td>
<td>- Proficient knowledge of the PassPort Accounts Payable, inventory mgt., purchasing, contract mgt., and financial integration, MSDS products. - Proficient in</td>
<td>PassPort System Administrator</td>
<td>Yes</td>
<td>No</td>
<td>Tim Stokes (training coordinator) Kim Schultz (purchasing and contract mgt.)</td>
<td>No</td>
</tr>
<tr>
<td>Inventory Mgt. Administrator</td>
<td>Person responsible for</td>
<td>User Role/Responsibility</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Administrator</td>
<td>managing, verifying, and maintaining the</td>
<td>User</td>
<td>Reviewing and approving security access forms for user access to the Passport MSDS module.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport System Administrator</td>
<td>knowledge of the</td>
<td>Passport</td>
<td>PeopleSoft Passport Administrator managing, verifying, and ensuring Passport access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>�</td>
<td></td>
<td>Passport</td>
<td>Pre-Requisite to Obtain Access: No.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>�</td>
<td></td>
<td>Passport</td>
<td>CBT Computer Based (Training) Pre-Requisite to Obtain Access: No.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>�</td>
<td></td>
<td>Passport</td>
<td>Business Owner Designation Pre-Requisite to Obtain Access: No.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>�</td>
<td></td>
<td>Passport</td>
<td>Approvals Level Pre-Requisite to Obtain Access: No.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>�</td>
<td></td>
<td>Passport</td>
<td>Certification Pre-Requisite to Obtain Access: No.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>PassPort Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>preferences, simple, and complex code tables for the PassPort Inventory Mgt. module. Administrator is also responsible for reviewing and approving security access forms for user access to the PassPort MSDS module.</td>
<td>inventory mgt., purchasing, contract mgt., and financial integration, MSDS products • Proficient in knowledge of the Peoplesoft financial product modules • Proficient in knowledge of the Hanford Business Structure (HBS) • Product specs. • Documenting end user requirements • Ad Hoc reporting • Security setup and maint. • MS Access • Crystal Report Writer • Maint. of users guides • Business</td>
<td>085040 PassPort Inventory Mgt. for Inventory Mgt. Specialists</td>
<td></td>
<td></td>
<td>White (inventory mgt.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Role/PassPort Security Profile</td>
<td>User Responsibility Description</td>
<td>PassPort Access/Functions</td>
<td>Training Certification Required for Classes</td>
<td>Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------</td>
<td>----------------------------------------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ABEND log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing lists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>User Role/HRIS Security Profile</th>
<th>User Responsibility Description</th>
<th>HRIS Access/Functions</th>
<th>HRIS Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Personnel Records Update User  | Update employee and job change information. Update hires, terminations, department changes. | • Personal Data  
• Employment  
• Job Data  
• Emergency Contact  
• Jobcode, grade and salary tables  
• Department table  
• Education  
• Applicant Hire | • Intro to HR  
• Intro to Benefits  
• Crystal Reporting  
• Query  
• PS/iVision  
• Process Scheduler  
• Recruitment  
• Position Management | None | None | Becky Calapristi | HR Security Access 
Administrator Approval and/or HR Management |
| Benefits User                  | Use and maintain employee insurance eligibility and options. | • Base Benefits  
• Personal Data  
• Employment  
• Job Data  
• Dependent/Beneficiary  
• COBRA Data | • Intro to HR  
• Intro to Benefits  
• Intro to Payroll  
• Crystal Reporting | None | None | Becky Calapristi | HR Security Access 
Administrator Approval and/or HR Management |
| COBRA – Inactive Employee Insurance Maintenance | Maintain the insurance coverage of inactive employees. | • Administer COBRA  
• Benefits Billing | • Intro to HR  
• Intro to Benefits  
• Intro to Payroll  
• Crystal Reporting | None | None | Becky Calapristi | HR Security Access 
Administrator Approval and/or HR Management |
<table>
<thead>
<tr>
<th>User Role/HRIS Security Profile</th>
<th>User Responsibility Description</th>
<th>HRIS Access/Functions</th>
<th>HRIS Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pension &amp; Savings User</td>
<td>Identify pension and retirement eligibility and benefit for employee.</td>
<td>Personal Data, Employment, Job Data</td>
<td>Intro to HR, Crystal Reporting</td>
<td>None</td>
<td>None</td>
<td>Becky Calapristi</td>
<td>HR Security Access Administrator Approval and/or HR Management</td>
</tr>
<tr>
<td>EEO User</td>
<td>Report EEO and Affirmative Action goals and status.</td>
<td>EEO Status, Personal Data, Employment, Job Data, Competency Management, Career/Succession Planning</td>
<td>Intro to HR, Crystal Reporting, Career/Succession Planning, Competency Management</td>
<td>None</td>
<td>None</td>
<td>Becky Calapristi</td>
<td>HR Security Access Administrator Approval and/or HR Management</td>
</tr>
<tr>
<td>HR Service Provider</td>
<td>View and report employee job history, compensation and disability. Update and maintain recruiting activity. Provide update direction to HR personnel records update users.</td>
<td>Applicants, job requisitions, recruiting, Personal Data, Employment, Job, Salary Planning, Base Benefits, Set up HGET training, Competency Management, Position Management</td>
<td>Intro to HR, Intro to Benefits, Crystal Reporting, Planning Compensation, Position Management, PS/n Vision, Recruitment</td>
<td>None</td>
<td>None</td>
<td>Becky Calapristi</td>
<td>HR Security Access Administrator Approval and/or HR Management</td>
</tr>
<tr>
<td>User Role/HRIS Security Profile</td>
<td>User Responsibility Description</td>
<td>HRIS Access/Functions</td>
<td>HRIS Recommended Training Classes</td>
<td>Training Certification Required for Production Region Access?</td>
<td>CBT (Computer Based Training) Pre-Requisite to Obtain Access</td>
<td>Functional Business Owner POC:</td>
<td>Approval Level Designation Required for Profile?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------</td>
<td>----------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
| HR Subcontractor User          | View and report compensation, employee job history, disability and recruiting activity. | • Applicants, job requisitions, recruiting  
• Personal Data  
• Employment  
• Job | • Intro to HR  
• Crystal Reporting  
• Recruitment | None | None | Becky Calapristi | HR Security Access  
Administrator Approval and/or  
HR Management |
| HR System Functional Administrator | Identify and maintain appropriate security access for users. Map data for system upgrades. Test software changes. Define user requirements. Provide training and help for database users. Set up and define new system functionality. Maintain production reports and system interfaces. | • All HR panels and tables  
• Overall HR security access  
• Manage database changes | • Intro to HR  
• Intro to Benefits  
• Intro to Payroll  
• Position Management  
• Crystal Reporting  
• Query  
• PSnVision  
• Manage Competencies  
• Recruitment  
• Planning Compensation  
• PeopleTools  
• Process Scheduler | None | None | Becky Calapristi | HR Security Access  
Administrator Approval and/or  
HR Management |
| Payroll User                   | Maintain payroll tables. For example, taxing, insurance, additional pay, earnings and deductions etc. | • Base Benefits  
• Tax Tables  
• Payroll Tables  
• Personal Data | • Intro to HR  
• Intro to Benefits  
• Intro to Payroll  
• Crystal Reporting | None | None | Didi Staudacher | Payroll Security Access  
Administrator Approval and/or  
Payroll Management |
<table>
<thead>
<tr>
<th>User Role/HRIS Security Profile</th>
<th>User Responsibility Description</th>
<th>HRIS Access/Functions</th>
<th>HRIS Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
</table>
| Payroll System Functional Administrator | Identify and maintain appropriate security access for users. Map data for system upgrades. Test software changes. Define user requirements. Provide training and help for database users. Set up and define new system functionality. Maintain production reports and system interfaces. | • All Payroll panels and tables  
• Overall Payroll security access  
• Manage database changes | • Intro to HR  
• Intro to Benefits  
• Intro to Payroll  
• Adv Payroll  
• PeopleTools  
• PS/n Vision  
• Payroll Year-End | None | None | Didi Staudacher | Payroll Security Access Administrator Approval and/or Payroll Management |
| Training User | Schedule and register employees into training courses. Bill departments for classes taken. Update training requirements. | • Scheduling and registration  
• TMX  
• Course Billing  
• Completed Training | • Crystal Reporting | None | None | Lucy Reed | Training Security Access Administrator Approval and/or Training Management |
<table>
<thead>
<tr>
<th>User Role/HRIS Security Profile</th>
<th>User Responsibility Description</th>
<th>HRIS Access/Functions</th>
<th>HRIS Recommended Training Classes</th>
<th>Training Certification Required for Production Region Access?</th>
<th>CBT (Computer Based Training) Pre-Requisite to Obtain Access</th>
<th>Functional Business Owner POC:</th>
<th>Approval Level Designation Required for Profile?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training System Functional Administrator</td>
<td>Run completed training reports.</td>
<td>Reports</td>
<td></td>
<td></td>
<td></td>
<td>Lucy Reed</td>
<td>Training Security Access Administrator Approval and/or Training Management</td>
</tr>
<tr>
<td>Training System Functional Administrator</td>
<td>Identify and maintain appropriate security access for users. Map data for system upgrades. Test software changes. Define user requirements. Provide training and help for database users. Set up and define new system functionality. Maintain production reports and system interfaces.</td>
<td>All training panels and tables</td>
<td>Overall training security access</td>
<td>Manage database changes</td>
<td>Intro to HR Crystal Reporting PS/n Vision PeopleTools</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>