SDDPC San Diego Data Processing Corporation	Procedure Owner: Unix Admin Dept	Effective Date: [Eff Date]	Identifier: PRO0581-019
Procedure Name: **Account Management**		Page: 1 of 5	Revision: Draft
		Prepared by: James Dorman	Approved by: [redacted]

DRAFT

1. PURPOSE

Provide general guidelines and procedures for Unix Account Management

2. SCOPE AND APPLICABILITY

This document covers Unix account naming conventions, uid and gid assignment, home directory location, and account creation and termination.

3. PROCEDURE

The following procedures will be used for Unix Account Management:

3.1 Information

The following additional information is pertinent:

3.1.1 Related Documents

a. Unix Admin Department Naming Standards document.

3.1.2 Forms

a. None

3.1.3 Audience

a. Unix System Administrators

3.1.4 Assumptions

a. The User is a Unix System Administrator.

b. Knowledge of AIX or Solaris

3.1.5 Approvals

a. None

3.1.6 Change Management Requirements

a. ?

3.1.7 Impact

What is the impact of not following these procedures?

3.2 Working With Accounts

3.2.1 Unix Account Policy

a. Every Unix user should have his/her own Unix account. Shared accounts are not allowed.

b. Unix accounts for applications should generally be locked, so no direct login will be allowed. Exception may exist.

3.2.2 Account Types

There are three types of accounts:

a. **System accounts**: those created by default in OS installation.

b. **User accounts**: accounts for real user

c. **Application accounts**: accounts for applications

3.2.3 Account Naming Convention

Currently, a user's Unix account uses the standard three character TSO name. As we're moving to first name initial plus last name convention for other account names, we'll evaluate and determine if the Unix account naming convention will be moving to the same direction.

Note: There's no defined account naming convention for application accounts.

3.2.4 Password Policy

a. The Unix account password should be 6-8 characters long, including at least one non-alphabetic character, and should not easily guessed. We may run certain programs to make sure users will choose a strong password.

b. Password expiration is not enforced, unless corporate requires.

c. Password should not be imbedded in any script in clear text.

3.2.5 UID Assignment

a. 0 – 100 reserved for system use

b. 101 – 999 application accounts

c. 1000 – 9000 user accounts

Assigned UID should be kept in **/sam/doc/uid**. When assigning UID to new account, the next available number should be used.

3.2.6 GID Assignment

a. 0 – 100 reserved for system use

b. 101 – 999 application groups

c. 1000 – 9000 other groups

Assigned GID should be kept in **/sam/doc/gid**. When assigning GID to new group, the next available number should be used.

3.2.7 Home Directory

The Home directory for user accounts is global, and is under **/home/<account name>,** and located on **nas3:/vol/vol1/home**. An **Automount map** has been created, so the user will be directed to their home directory no matter which machine they logged in.

The Home directory for application accounts may be local, depending on the application requirement. However, a global home directory is preferred.

3.2.8 Account Information

User account information is kept in an Oracle table. The following information is kept:

AccountName	Account name
Password	Encrypted password
UID	UID
GID	GID
Name	Name of the sponsor. For user accounts, this should be the user's name (cn from LDAP directory). For application accounts, this should be the description of the application
Sponsor	Sponsor's ID. For user accounts, this is user's TSO. For application accounts, this is application owner's TSO
HomeDirectory	home directory
Shell	default shell
Status	Active or Nonactive

Additional information can be obtained from the LDAP server.

There's a second table that keeps track of which user account is allowed on which machine.

The **/etc/passwd** and **/etc/shadow** entries are generated by script automatically from the information in Oracle table

3.2.9 Account Creation

a. The Unix account for a user should only be created after the corresponding LDAP entry is created.

b. Account creation can be initiated by the user himself, by his direct supervisor, or by Human Resource personnel.

c. When requesting a new account, a user only needs to provide his/her TSO. For an application account, a description of the application, and the sponsor's TSO are also needed. A list of machines that account needs to be created on is also required.

d. Use account management script (to be determined) to create account, The script only runs on sheera. It'll create the account, and email the password to user (sponsor). Application account is locked by default. It can be unlocked, and assign a password on sponsor's request.

3.2.10 Account Termination

A user's account should be disabled upon the user's termination, or when he/she no longer needs it.

A account management script should be used to disable/delete an account.

On a user's termination, the user's account should only be disabled, not deleted. The account should be kept for 3 months. The account's home directory should also be kept. After a 3 month period, the account and home directory will be deleted,

4. NOTES

4.1 Revision History

Date	Revision	CR No.	Description	Author
12/28/2001	1st Draft		Initial Draft	Patrick Zhang

4.2 Diagram

Not Applicable