SOP SETTING UP USERS AND PRIVILEGES

MEDATECH

FUTURE PROOF YOUR BUSINESS

MEDATECH

FUTURE PROOF YOUR BUSINESS

SOP SETTING UP USERS AND PRIVILEGES

TABLE OF CONTENTS

AIM

- To define new users.
- To manage entry passwords.
- To manage privileges.

The processes described in this document are only to be performed by the system manager ("tabula").

PROCEDURE

STAGE ONE: DEFINING USERS

1. Run the Add New User program.
2. In the User Name column, record the name the user will use to enter the system.
3. Record the user's Full Name in order to identify the operations he/she performs.
4. Record a unique Social Security No. for the user.
5. If the user belongs to an existing user group, select the relevant group leader in the Privilege Group Leader column. The new user will receive the system privileges defined for the group leader. If you leave this column empty, the user is considered a group leader, and you will need to define privileges for him/her in the Privilege Explorer (see Stage Four).
6. To view the program's results, enter the Users form and retrieve the new users.

STAGE TWO: DEFINING GROUP LEADERS

Group leaders are defined in the system as regular users and are used to assign the same privileges to a group of actual users. It is recommended to define fictitious users as group leaders (e.g., "Marketing", "Purchasing").

- Perform the steps in Stage One, but leave the Privilege Group Leader column empty.

STAGE THREE: LINKING USERS TO GROUP LEADERS

After defining group leaders, link each user to the appropriate leader, and the user will "inherit" the leader's system privileges.

1. Enter the Users form.
2. Retrieve each user, and select the desired Group Leader (Privs) from the Choose list.

RESULT

Each user "inherits" privileges from the group leader to which he/she is assigned.

STAGE FOUR: ASSIGNING PRIVILEGES TO GROUP LEADERS

1. Run the Privilege Explorer and select the desired group leader.
2. The explorer opens a "tree" of entities in Priority, which parallels the main systems menu. Define privileges for each possible operation in the menu:
    - Menus
    - Forms and Sub-level forms
    - Activations (e.g., printouts, programs)
    - Form columns (fields)

    Next to each entity, a symbol appears representing the level of privilege assigned to that entity:

    - W - Full Access (Write and Update)
    - R – Read only
    - X – No access (the item will not appear in the menu)
    - ! – Undefined entity

    Symbols appear in green if all privileges beneath the entity in the hierarchy are assigned the same privileges and in grey, there are different privileges on the same level. For example, if you assigned full access to all entities in the Sales Order menu, a W appears in green. IF you change the privilege assigned to the Financial Status of Orders, form to read-only (R), the colour changes to grey.

    Important: The symbol! usually appears for new entities (e.g., menus, forms, form columns, programs) added to the system as private customizations or version upgrades, for which privileges were not assigned to group leaders. To prevent this from happening, assign the necessary privileges at all levels.

3. Continue "opening" the various menus until you reach the desired entity.
4. Right-click the entity title, and select the appropriate privilege from the pop-up menu:
    - Grant Read Privilege
    - Grant Write Privilege
    - Revoke Privilege - (prevent the user from seeing this entity)

    Note: The initial privileges defined for a menu or entity are automatically applied to any sub-menus and or entities at lower levels in the explorer (e.g., if you assign write privileges to the Customer Invoices menu). However, if the privileges for a menu or entity ae later modified, these modifications will not automatically override any privileges that were assigned directly to sub-menus and or entities at a lower level in the Explorer. If you want modification privileges for a given menu

or entity to be applied automatically to all sub-menus and or entities at all lower levels, select the Override option in the upper Edit menu.

5. To define mandatory columns in a given form, or hide columns, right-click the desired form (or sub-level form) and select Form Columns. Flag the appropriate option for the desired column:
    - Mark as Read Only
    - Mark as Mandatory
    - Hide
    - Give Full Access
6. To change the level of system warnings (i.e., to change warning into errors, or vice versa), or to cancel a message, right-click the desired form and select Form Warning Messages. Flag the appropriate option for the desired form:
    - Error Message
    - Warning Message
    - No Message.
7. Assign the relevant privileges to all undefined entities. Run the User Privs: Entities Not Treated report to identify new entities for which no privileges were assigned. Use this report after upgrading to a new version.
8. To authorise the privileges for a given group, select Apply Changes from the explorer's File menu. The system will automatically authorise the defined privileges.
9. To copy privileges from the current group leader to another, right-click the entity in question and select Copy to Other Users. You can copy the entire main menu or part of it, to one group leader or to several at once.
10. To copy privileges from the current company to another, right-click the entity in question and select Copy to Other Companies. You can copy the entire main menu or part of it, to one company or to serval at once.
11. To apply the new privileges, leave and reenter Priority.

STAGE FIVE: VIEWING THE PRIVILEGES DEFINED IN THE EXPLORER

1. You can view the defined privileges in the following query forms:
    - Privileges for Group/User
    - Form Priv Restrictions + Warn Msgs
    - Privileges per Entity
2. Run the following reports to check the privileges:
    - Discreps in User Privilege Tree – Displays all entities assigned contradictory privileges. If an entity that appears in two menus is assigned a different privileges in each menu, the least restricted privilege will apply.

      Example: The Customers form appears under both the Customers menu and the Marketing Menu. If a group leader is assigned read privileges for the form in the first menu and write privileges for the form in the other menu, the user will receive write privileges for that form.

- Column Privilege Restrictions – Displays the names of users assigned read privileges for certain form columns and the columns that are read-only for all users.

STAGE SIX: MANAGING PASSWORDS

CHANGING A PASSWORD

1. Run the Assign Password program and retrieve the desired user.
2. Record a new Password. Note: Use this program for new users, or when existing users do not remember their password. In any other case, it is better to have users change their own passwords by running the Change Password program from the Upper File menu.

DEFINING A PASSWORD POLICY

1. To require users to enter the system with a password, run the Set Password Policy program.
2. Specify the number of days the password will be valid and the minimum number of characters to be used.
3. To require the use of complex passwords (comprised of digits, upper-case letters and lower-case letters, flag the Complex Password column.

RESULT

When users first enter the system, they are asked to define a password, which they will then the user (together with their username) to enter the system from now on.

STAGE SEVEN: DEFINING A USER AS INACTIVE

1. Enter the Users form.
2. Retrieve the desired user and move to the User Permissions sub-level form.
3. Flag the Inactive User column (in the Permissions tab).

RESULT

An inactive user will not be able to log in and record data in Priority, even if they are still linked to a privilege group.