

## **MIS Security (SEC)**

### ***Overview***

MIS Security, hereafter referred to as SEC, enforces application security - and not at the expense of flexibility. That is, maintaining SEC data is treated as one part/module of the whole software application, although SEC is the one that determines the manner in which to access and use any of the other modules in the application.

In other words, the SEC module is a solid base to MIS software application. Any upgrade or additional module will be built on it, and the same SEC screens will be run to secure these new upgrades or modules. Besides this stability feature are others listed below showing the power and advantages of SEC.

### ***Features***

- SEC is menu-driven and easy to manipulate, with hints guiding the System Administrator (SA) to specify/modify security for the users across the modules.
- SEC has a user-friendly graphical interface which facilitates the completion of the SA's tasks.
- SEC inherits bilinguality from MIS application software. Descriptions, names and titles may be specified and viewed in Arabic, as well as in Latin characters (English, French, etc.)
- SEC maintains information about each user, including password and status. That is, a defined user cannot be removed; but his/her status may be set to inactive, preventing him/her from accessing any module of the software application. Along with an active status, valid user ID and password must be input in order to have access to the system.

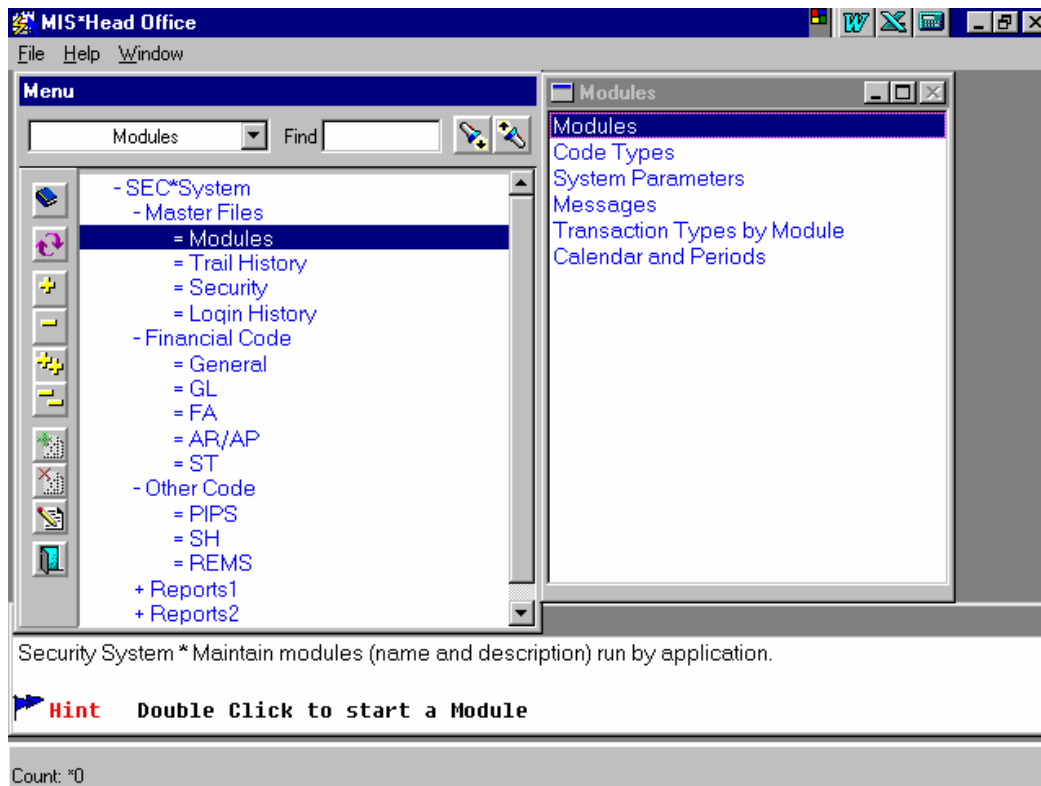
- SEC also trails the changes on password for every user, giving the System Administrator the possibility of auditing this trail information. In addition, the SA may want to force the users to change their passwords within a maximum of n-days. If n-days is defined to the system, a user with an old password (latest change since more than n-days) will not be able to access the system unless he/she requests a password change from the System Administrator.
- SEC provides the System Administrator with control on the screens and reports of the modules. For screens, the SA is able to change their text labels; for reports, he/she is able to change their parameter text and column heading text.
- SEC also provides the System Administrator with control of error messages and warnings. He/she has the facility to change the text for all messages generated by the application.
- SEC enables the System Administrator to associate a hint message with a field in a screen.
- SEC has a core menu structure which includes all the options of the modules in the application software system. Options are grouped into menus, which also may be grouped into higher level menus.
- SEC takes into consideration 3 classes for security, the privileges of the higher including those of the lower. The lowest class [User] is a user-local security where one is only able to manipulate data owned by oneself. The higher class [Group] is a user-role security where one is able to manipulate data owned by oneself or by one of the same role/group. Finally, the highest level [All] is a super-user security where one is able to manipulate any data, disregarding its ownership. Note that the owner of data is the user who first created it.
- SEC also considers 5 types of actions to be secured:
  - \* [Add]: add new data
  - \* [Modify]: change data
  - \* [Delete]: remove data
  - \* [Query]: view data
  - \* [Trail]: audit changes on data

- SEC joins the 3 classes with the 5 types of actions to base its security control on 13 different rights, which combinations are considered as security levels. The latter may be specified by the System Administrator, activating a set of rights:

* [Add Data]:	right to add new data
* [Modify Own Data]:	right to change self-owned data
* [Modify Group Data]:	right to change group-owned data
* [Modify All Data]:	right to change any data
* [Delete Own Data]:	right to remove self-owned data
* [Delete Group Data]:	right to remove group-owned data
* [Delete All Data]:	right to remove any data
* [Query Own Data]:	right to view self-owned data
* [Query Group Data]:	right to view group-owned data
* [Query All Data]:	right to view any data
* [Trail Own Data]:	right to audit self-owned data
* [Trail Group Data]:	right to audit group-owned data
* [Trail All Data]:	right to audit any data

- SEC guarantees function security control. In fact, it enables the System Administrator to assign security levels to different users for each option of the menu structure. In other words, one option - be it screen, report or menu, may be run by more than one user, not necessarily with the same set of rights. In addition, one user may run various options also not necessarily with the same set of rights.
- SEC guarantees row security control. Thus, the System Administrator is able to assign a security level to a user on certain rows of data. The function security would be enforcing the ownership criteria in combination with the types of actions; the row security would be enforcing a flexible SA-defined criteria together with ownership and types of actions. A good example would be the function "account balance" in a GL module - a user would have the query right on specific accounts only, preventing him from viewing all accounts balances.
- SEC guarantees field security control, as specified by the System Administrator, still using the security level concept. Field security is enforced on the top of function security and row security. Thus, first the function security is checked, then the row security, and finally the field security. So there may be for instance a user able to query a list of data without viewing one column in that list. The reason for that is that he would have a query right on that data, but not on that column/field. Another example would be to give a user permission to update data through some function/screen, while preventing him/her from modifying a specific item (which may require higher authority).

- SEC is flexible in terms of history keeping; there is no need to upgrade or change a program in order to trail certain information. The System Administrator would indicate an item to be trailable, following which history is recorded for every change of that item (be it a modification or a deletion).
- SEC provides on-line audit trail facility on items/fields provided that the item is trailable and that the user has the appropriate field security level.
- SEC facilitates the identification of a user by grouping all the above settings by user in one place/option.



MIS\*Head Office - [MSG\_DEF]

Action Edit Block Field Record Query Window Help

22-11-1997

System Error Messages...

Num	English Message	Arabic Message	Modul
809	Argument Number is null for argument of type.	لا يمكن أن تكون المعادلة خالية لهذا العنصر.	SEC
810	No such argument \$.	لا يوجد هذا الرمز \$.	SEC
811	No such Argument &.	لا يوجد هذا الرمز &.	SEC
812	There is no argument type for.	لا يوجد رمز للعنصر.	SEC
813	Error in parsing formula.	خطأ في كتابة المعادلة.	SEC
814	Failure in parsing formula.	فشل في كتابة المعادلة.	SEC
815	Duplicated: Default location already specified f	مكرر - تم مسبقاً تعريف موقع اولي لمركز المخزون	ST
816	No such code for category.	رمز الصنف غير معرف.	ST
817	No such code for costing.	رمز التسعير غير معرف.	ST
818	No such code for height unit of measure.	رمز وحدة قياس الأرتفاع غير معرف.	ST
819	No such code for width unit of measure.	رمز وحدة قياس العرض غير معرف.	ST
820	No such code for weight unit of measure.	رمز وحدة قياس الوزن غير معرف.	ST

Count: 210 ^ v