# COP 4005 – Project Instructions – SECURITY Management

Using the STARSOrg application partially developed in class, you will complete the security management functionality. Each user of the application must have a set of login credentials (UserID and Password), and each user must be assigned to a specific security role.

Tables you will need to use:

* MEMBER
* SECURITY
* AUDIT

For each table, you will need to:

* Create classes as needed. Follow the patterns for classes as shown in the class samples
* Create appropriate stored procedures for the necessary operations

The following functionality is required:

* Add a login screen and require all users to log in. Login should be the first action required when the program starts. Login should only be required once.
* Each successful and unsuccessful log-in attempt must be saved into the AUDIT table.
* Login screen should provide the ability for a user to change his or her password.
* Administrator screen that allows a user with admin security privilege level to assign initial login credentials and security privileges to a new member, or to reset a member’s password.
* Must provide to all other screens information about the currently logged in user, including the PID and the security role held by the logged in user.
* Must allow log-in as a guest (whose actions will be limited), with no PID, user ID or password required. This access must also be audited. Create a guest member record whose PantherID is “0000001” for this purpose.
* Must have a member account must be created with ID value of 9999999 to represent unsuccessful log-ins
* Security privilege levels will be hard-coded into the program, and consist of the following values:
  + ADMIN
  + OFFICER
  + MEMBER
  + GUEST

Notes:

* It will probably be easier to integrate the Security portion into the entire project last. Other team members should get their functionality and new screens working together, then add the security into the project in a consistent way (common procedures/functions/class objects).