Detailed Use Case (**Scenario #1**)

|  |  |
| --- | --- |
| **Use Case Textual Description** | |
| **UC-ID** | 0.0 |
| **Name** | User Authentication |
| **Description** | User authentication is identified to be key to the security of the system. Not only does it protects the system from unauthorized usage, it also differentiates the intended user from three different levels of system permission through a logging in process. Password change and reset are other options on this menu. |
| **Actor(s)** | Operator, Manager, System Administrator |
| **Main Scenario** | 1) At user authentication screen, user enters his ID and password  2) Authentication success, user enters his permitted menu  3) User choose to quit, his account is logged out back to user authentication screen  4) User choose to change password, he is prompted to enter his ID, old password and new password  5) Authentication success, password is changed  6) User choose to reset password, he is prompted to enter his ID and staff email address  7) Authentication success, random new password is generated and sent to his staff email |
| **Sub Scenario** | 1) At user authentication screen, user enters his ID and password  2) Authentication failure, user will be prompted to enter his password again  3) After three fails, user’s account will be locked, he may not attempt anymore  4) System administrator will be notified of a locked account |