***Login - Use Case***

### ***Goal***

A user logs in to authenticate and determines their role (Customer or Admin.) in the system.

### ***Pre-Conditions***

* The user has already created an account.

### ***Flow of Events***

#### Basic Flow – A user attempts to log into the System.

1. This use case begins when a userfirst connects to the system.
2. The *system* displays the required authentication information (see login data definition).
3. The user enters their authentication information.
4. The *system* attempts to authenticate the entered user information.
5. The *system* determines the user’s role (see Additional Detail below).
6. The Use Case Ends

### Exception Flow #1 – User fails authentication

1. This flow begins when the userenters an invalid Email and/or password (reference Basic Flow Step 3)
2. The *system* describes the reasons why the User failed authentication.
3. The system prompts theuser to enter valid information.
4. The Basic Flow continues where the user enters authentication information (see step 2 of the Basic Flow).

### ***Additional Detail***

* The user’s role (Customer or Admin) is determined by checking the entered Email with the saved system information.

### 

### ***Special Requirements***

* Security - SEC1 - The system must authenticate all users using a login ID and password.
* Security - SEC2 - The system must not grant authorized access to unauthorized users. If a user fails 3 consecutive attempts at accessing the system, the user will be locked out for 10 minutes.
* Scalability - SCA1 - The system must handle up to 1000 users at one time.

### ***Post-Conditions***

* The user has been successfully authenticated into the system.

### ***Analyst Notes***

* N/A