# Sprint 1 - Feature list for User Interface Module:

1. Allow three types of users – **administrator**, **manager**, and **regular user** (accountant) to login to the system;
2. The administrator user should be able to create users and assign roles;
3. The administrator user should be able to update information about a system user;
4. The administrator user should be able to activate or deactivate each kind of user;
5. Each kind of user should be able to log in to the system once credentials are created in the system
6. The login username, picture, should be displayed clearly on the top right corner of the login page once they have successfully logged into the system;
7. The login page should have:
   a. A text box to enter the username
   b. A textbox to enter a password which will be hidden as the user keys in the password
   c. A submit button
   d. A forgot password button
   e. A create new user button
   f. A **logo** which will be displayed on all the pages of the application
8. The **create a new user** button will be used if the user is accessing the system for the first time. Clicking this button should display a user interface where the user will provide personal information such as first name, last name, address, DOB, and click submit to request access to the application. The administrator should receive email request and must approve or reject the request. If approved, an email should be sent to the user with a link to login to the system;
9. A button for **forgot password**. If this button is clicked, the system should prompt the user to enter email address and user id the person provided when his credentials were created in the system and ask security questions to allow him to supply new password;
10. Passwords must be a minimum of 8 characters, must start with a letter, must have a letter, a number and a special character, if this requirement is not satisfied, display at appropriate error message;

11. Password used in the past cannot be used when password is reset;
12. Password must be encrypted;
13. A maximum of three wrong password attempts should be allowed after which the user should be suspended;
14. All login information must be stored in database tables;
15. Three days before a password expires, the user should receive notification that the password is about to expire;
16. The administrator should have a report where he can view all users in the system without going straight to the tables;
17. The administrator should be about to suspend any user from a start date to expiry date such as if the person is on an extended leave;
18. The administrator should get a report of all expired passwords;
19. The administrator should be able to send email for any user from within the system;
20. A username should be made of the first name initial, the full last name, and a four digit (two-digit month and two digit year) of when the account is created;