**Business Requirements Document for Login page**

**Customer: GMIT Credit Union**

1.0 Display company logo on the left hand side of login panel

2.0 Display Company name top centre of login panel

3.0 To successfully login to an account a valid email and password must be entered.

4.0 User name will be the users e-mail e.g. "username@yourdomain.com".

5.0 The password will contain between 8 and 12 alpha and numeric characters with one alpha character being a capital

6.0 There will be an option for user to reset password if it is forgotten

6.1 Details of new login ID’s emailed to client

6.2 Reset credentials will be emailed to user

7.0 Use social login buttons to “Log In With Twitter” or “Log In with Facebook

8.0 When you login to your account, a new "session" is created. A session has an "inactivity timeout" period of 3 minutes. This means if you don't click a link or button on a page within this amount of time, the session will expire, and user will have to login again to continue.

9.0 The option to remember passwords and user name will be available allowing passwords to be stored in the browser using cookies

10.0 For new user who do not have an account there will be a “Join Now” option.

10.1 The new password will be emailed to the user.

11.0 Users will be told exactly where their credentials are incorrect. If the user name is incorrect the entry field will be highlighted by a red box with the following error message displayed in red

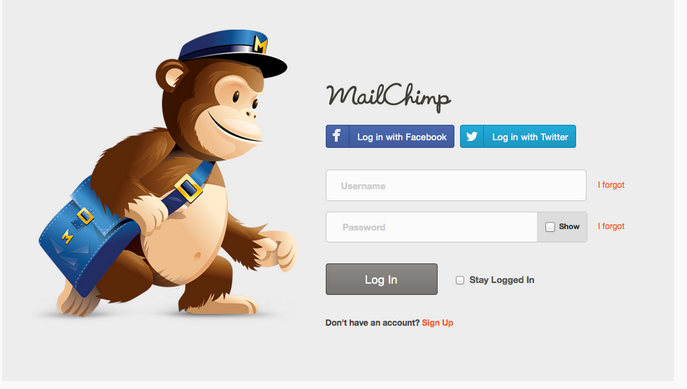
Sorry we couldn’t find an account with that user name

If the password is incorrect the entry field will be highlighted by a red box with the following error message displayed in red.

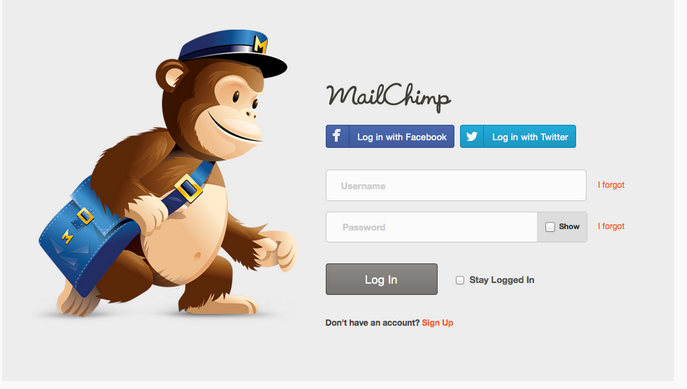
Sorry we couldn’t find an account with that user name

12.0 Ability to analyse visitor traffic research login patterns using Analytics to determine the number of login failures

13.0 Login screen background. As detailed in mock-up below



14.0 Login screen form settings. As detailed in mock-up below



15.0 User name and password validation checks. (example of vague requirements)

16.0 Back-office validation e.g Session management requirements

17.0 Security Requirements

17.1 Login page must be secure therefore encryption of login information is required.

17.2 Sensitive information e.g. usernames, passwords, names, addresses, phone numbers, and credit card details stored in an application’s database must be secure