Deliverable No. 1

LOGIN MODULE

Minimum Requirements for Login Module

Registration Sub Module/Sign Up. The module must be able to register new users that will capture the important user information such as, but not limited to, last name, first name, middle name, email address, user name.

- ✓ Password can be defined by the user or system generated. For the system generated password, the system shall be able to prompt the user to change the password during the first time the user logs in the system.
- ✓ For the input-type password, the following shall be considered:
  - Password must at least eight (8) characters long
  - Must have at least one (1) numeric and special character.
  - At least one (1) capital letter.
- ✓ Use of captcha is preferred but not mandatory.

Activation of Account. After registration of user account, the user must be able to activate the user account before it can be used. This can be done thru the use of email address and/or contact number provided during the registration.

Password Recovery. The module must have the mechanism to recover password. This can be done either **Forgot Password**, provide an answer to a **Secret Question**, or sending a One-Time Password (OTN) thru mobile number provided during the registration.

Change Password. The system must allow the user to change the password. The system must alert the user when the password needs to be changed. The user can waive the changing of passwords.

Notifications. The module also provides some notifications for the administrator or regular users to understand what is happening. All the messages could be customized with several placeholders provided by the module. The following are list of notification options:

- ✓ **Display last login timestamp**: Displays when a user last logged in at each successful login.
- ✓ **Display last access timestamp**: Displays when a user last accessed the site at each successful login.
- ✓ **Notify the user about the number of remaining login attempts**: Warns the user about the remaining attempts available before the account is blocked.
- ✓ **Disable login failure error message**: Selecting this option will show no error message at all, so user will not be aware of unsuccessful login attempt, or blocked account messages.

- ✓ **Send an email message to the admin about blocked accounts**: An email could also be sent to the administrator, each time an account is locked.
- ✓ **Send email message to the admin about suspicious login activity**: An email could also be sent to the administrator, whenever suspicious activity being detected in the login form submissions. When a determined value (threshold) of invalid login attempts is reached, an email will be sent.

Ongoing attack detection. The system is able to detect if a password-guessing or brute-force attack is being performed against the login form. Using a threshold value, you may instruct the module to alert (using a watchdog message, and optionally send an email) the administrator user when the number of invalid login attempts reaches the threshold value, used to early react on unexpected login attempts.