**5.6. Management of Secret Authentication Information of Users**

1. All Organization’s systems shall require identification and authentication through a proper secret authentication information method (e.g., passwords, token IDs, smart cards or biometrics).

2. Prior to allowing user access to any system or application, a password authentication method shall be implemented as follows:

a. Password shall be a minimum of 8 characters length for normal users and 12 characters for IT administrators (e.g., system admin, application admin, DB admin and network admin).

b. Password shall be combination of at least three of the four followings:

▪ At least one lower case alphabetic character (a-z)

▪ At least one upper case alphabetic character (A-Z)

▪ At least one number (0-9)

▪ At least one special character (e.g., @#$%^&\*()\_+|~-=\`{}[]:";'<>/)

c. Passwords shall not contain user ID.

d. Passwords shall contain no more than two identical characters in a row and not made up of all numeric or alpha characters.

e. Blank password shall not be allowed.

f. Users shall be required to change their password immediately after their first login to any system (i.e., It shall be configured to prompt a user to choose another password before continuing with his session). g. User account shall be locked fort 3 minutes after 3 unsuccessful attempts:

h. Password change shall be enforced (by the operating system or the application) at least every 90 days. Re-use of the same password shall not be allowed.

i. Initial password shall be only used one time (i.e., it shall be valid only for the involved user’s first login) and shall be expired at 23:59:59 of the date issued.

j. Password shall be stored and transmitted in protected (e.g., encrypted or hashed) form, if possible.

3. Passwords shall be immediately changed if there is any suspicion of password compromise; and this shall be reported immediately