**Password Policy**

1. **Purpose**  
   To provide guidance and direction to our employees about password creation, use and account management. Passwords are key to keeping your account secure and are the first line of defense to protect our sensitive company information. This policy covers both users and services managed by system administrators.
2. **Policy**
   1. It is out company’s policy that users shall establish and maintain strong passwords to prevent malicious actors from easily guessing the password;
   2. Passwords shall be different from the previous ten;
   3. Passwords shall be made up of a mix of numbers and letters with special characters such as (!@#$%^&\*()\_+) and a mix of upper and lowercase characters;
   4. Passwords shall be a minimum of 16 characters long;
   5. Passwords shall not be written down on a sticky note, displayed on public-facing screen or under a keyboard;
   6. Passwords shall not be shared with anyone;
   7. Passwords shall be stored as hashed values using the bcrypt encryption algorithm;
   8. In the event of a password breach, the account will be temporarily locked to ensure security. An email will be sent to the user with instructions to reset their password promptly;
   9. After five consecutive failed login attempts, the account will be temporarily locked for 24 hours;