Goldmine Stocks Pvt. Ltd.

Password Policy

The login process for our trading application and other web based applications is fully secured. Credentials are sending encrypted in a public key generated by the OpsEngine. This public key is re-generated every session. Passwords are saved at the backend in an encrypted manner. Goldmine does not have access to user/client passwords and it user's own liability if any loss/damage arises due to any technical error/glitches, if user has not set strong password of its login. The employees of the organization do not have access to user passwords details and Ex-employee's passwords do not be reused across multiple accounts and/or list of passwords not be stored on the system.

-
- The new Password should be minimum of 6 / 8 characters
- It should contain atleast one capital alphabet, one small alphabet, one numeric and one special character.
- All applications must be login after two factor authentication (2FA) i.e. OTP or Verification code or Biometric etc.
- For IBT/Mobile trading application users an additional 4 digit numeric verification code and Back office application user enter OTP as a part of two factor authentication
- Trading Application password will be expire every 180 days and/or our own discretion it's changed from time to time
- User login shall lock after 5 invalid login attempts
- New password must be different from previous 5 passwords
- User shall not be allowed to set the default password as new password
- User must be reset his/her default password with user of his login id and PAN

Don'ts

To avoid your account from getting hacked, here's a list of worst passwords you should avoid

- Avoid using 123456, the most common of all passwords
- Switching a letter to a symbol like p@ssw0rd! too is an obvious trick that hackers know
- Password cracking programs contain every type of these combinations in every language
- Use something obscure and avoid using names of your favourite sports team or pop culture references
- Using single words like sunshine or monkey and adding a number or punctuation at the end doesn't make for a strong password. Instead, use a phrase or sentence to make your password stronger
- Avoid using common password such as 111111, abc123, Abc@123 or 654321
- Do not share your login information to any one and also do not save in your local system

Dos:

What makes a password strong?

- Combining unrelated words
- Using an entire phrase and changing some of the letters to special letters and numbers
- Use a combination of upper and lower case letters, symbols and numbers
- The longer your password, the stronger it is
- Use different passwords for every account

****