Rudra Shares & Stock Brokers Limited

Policy for Two Factor Authentication

This is with reference to SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, on Cyber Security & Cyber Resilience framework for Stockbrokers, wherein all Trading Members were required to mandatorily implement two-factor authentication on application offered by Members to customers through Internet Based Trading (IBT) and Securities Trading through Wireless Technology (STWT).

Detail regarding current two factor authentication facility implemented in our in-house developed IBT & STWT application RUDRA MINT & empanelled vendor application MoneyMaker Solo (IBT) and MoneyMaker Handy (STWT) -

1. We are compliant with 2-factor authentication (2FA) procedure in accordance with aforesaid SEBI circular - ***Yes***
2. Details :

Knowledge Factor		**Possession Factor**	
User ID/ PW	*Yes*	Biometric	*Yes*
DOB	*No*	OTP	*Yes*
Mobile PIN	*Yes*	Authenticator Apps	*No*
PAN	*No*	Security token	*No*
Others(Specify)	*No*	Other (Specify)	*No*

Procedure in brief for 2-factor authentication (2FA) on application offered by us to clients through Internet Based Trading (IBT) and Securities Trading through Wireless Technology (STWT).

Brief comments:

Currently this is the login at Rudra -

web ,mobile, exe
==========
userid & password --- compliant with knowledge factor

2FA - OTP (1st time login or fallback mechanism if mobile or authenticator app lost) or biometric (mobile) or TOTP (web/exe/mobile) --- compliant with possession factor

In cases, where biometric authentication is not possible, Members shall use both the aforementioned factors (Knowledge factor and Possession factor), in addition to the user ID, for 2-factor authentication (2FA). It is to be noted that the above mentioned authentication shall be implemented on every login session by the client to IBT and STWT.

Security: Password Policy –

BROWSER login process is fully secured. Credentials are sent encrypted in a public key generated by the OpsEngine. This public key is re-generated every session. Passwords are stored as MD5 hash.

Log-in password policy: To log-in in system, application will ask for login password and 2nd factor verification code.

a.Login Passwords expire every 180 days.
b.Login Password lengths are between 6 to 12 alpha-numeric characters.
c.Login Password Last three lapsed passwords are not allowed as new passwords.
d.Three consecutive failed login attempts lock the user.
e.System will ask to compulsory change password and verification code on the very first attempt.
f.Login Password & User-ID cannot be same.
g.2nd factor verification code 4 digit numeric only
h.User can change 2nd factor verification code any time as per user requirement.
i.Users can not use last Five used passwords.
j.Users can define the second authentication system as verification code, MPIN, Pattern lock, Face unlock system and PIN as allowed by devices (in case of STWT).

****