

Our Privacy Policy

Protection of Security Code(s)

The Client shall immediately notify the Member in writing, delivered via-e-mail and Registered AD, if the Client becomes aware of any loss, theft or unauthorized use of the Client's Security code (s) and account number or any failure by the Client to receive the confirmation of an execution including the contract note for the same; or any receipt by the Client of confirmation of an order and/or execution which the Client did not place; or any inaccurate information in the Client's account balances, securities position, or transaction history. In the case where the Client notifies such loss, theft or unauthorized use of the Client's Security code (s) password and account number to the Member, it shall suspend the use of the account of the Client, however the Client shall be responsible and liable for all transaction that are carried out by using the Client password. When any of the above circumstances occur, neither the Member nor any of its officers, directors, employees, agents or subsidiaries will have any responsibility or liability to the Client or to any other person whose claim may arise through the Client with respect to any circumstance described above.

Password Protection

We give you a unique user name and two passwords for transaction purposes. When you place an order we ask you for the transaction password, which authenticates your identity from our highly secured database. The system also has a feature, which automatically expires your transaction password in 30 days. This would mean we force you to change your password every month for ensuring high security for all your transactions. You can also change your password online at any time. In addition, you can use the Log Off button located throughout the site to securely exit your account without closing your browser.

Internet Scanners and Intrusion Detection System

The system maintains a database of attack signatures which is continuously updated and against which it will scan all incoming traffic to detect any malicious activity or hacking attempts into the site. In the event of a possible attack, it will terminate that session, log the attack details and also alert the administrators Identity Protection

Please do not reply/respond to any communication, including email, SMS or phone call informing you that your accounts will be closed unless you provide your personal information by responding to such communication or other email address/website/mobile number/phone number, or any communication requiring furnishing of any information personal or otherwise, and representing to be from CSL.

Avoid sending or furnishing personal and financial information on email. Also prior to providing any information (financial or personal) on a website, verify the bonafides of the

website, its address and of the owners/operators of such websites. Make sure that the URL (Uniform Resource Locator) that appears in the “address” or “location” box on your browser window is the one you wish to access.⁰⁷

Surveillance

PINAKINI SHARE & STOCK BROKERS LTD., has a very scientific risk management system in place. The company has a separate surveillance and monitoring department, where highly efficient and experienced personnel are in charge of close monitoring of terminal operations throughout the trading hours. Each and every branch/franchisee is under continuous watch as regards exposures, margins, timely payment of cash and shares, turnover, mark to market profits/losses and so on.

If you do not agree to any of the terms mentioned in this agreement, you should exit the site.