At Crowe Horwath, we are committed to protecting the security and confidentiality of your personal information so as to provide you with a safe and secure online environment. Our mobile application, enoVestor uses commercially proven security hardware and software products. These security products include routers, firewalls and secure operating system to safeguard your interest.

All connections must pass through at least one router and one firewall to gain access to the server. The firewall checks for the appropriate source address and restricts unauthorised access to the appropriate server.

Additional technical security features include Verisign digital certificates, 256-bit encryption, one-way hashing of all user passwords and automatic logoff after 10 minutes of inactivity.

Apart from the security measures put in place by Crowe Horwath, you play an equally important role in ensuring your online account information is not compromised.

Ten Critical Security Tips

1. To keep your information private, create a strong password for your mobile phone and set your screen to auto-lock within five minutes.

2. Update us immediately when you change your mobile number for receiving One-time Password (OTP) via SMS.

3. Update us immediately when there is a change in your contact details such as mobile number and email address for the purposes of receiving SMS alerts or email notifications.

4. Do not share your login credentials with anyone.

5. Do not install mobile apps from unknown sources (other than Google Play Store or Apple App Store).

6. If there is an update for your device from legitimate sources such as Google Play Store or Apple Play Store, install it. New updates are sometimes used to fix bugs and address security vulnerabilities.

7. Install reliable antivirus software on your mobile device and keep any security patch and antivirus software up-to-date.

8. Do not click on hyperlinks provided in mobile messages if you are unsure of the source.

9. Do not act on any instructions provided in unfamiliar pop-up screens which prompt you to provide your login credentials.

10. Log out from your mobile app session after use.