2FA Risk Awareness Statement

1. **What is 2FA?**
   2FA (also known as two-factor authentication) is the verification of a user's online identity.

   The current practice used by financial institutions in Singapore is the provision of a unique One-Time Password (OTP) to their clients. This is also practiced by KGI Securities. When a KGI Securities client wishes to access an online service by KGI Securities, the client is required to enter an additional unique OTP, which is generated on demand through a token device.

2. **What is the purpose of 2FA?**
   The key objectives of 2FA are to enhance the overall security of the client authentication process and to protect the integrity of client account data and transaction details. In doing so, client confidence in online trading systems will be boosted.

   Furthermore, 2FA is a useful tool against cyber attacks targeted at financial institutions and their clients.

3. **Is 2FA compulsory for trading through KGI Securities?**
   At this point in time, 2FA is not compulsory for trading through KGI Securities. That said, KGI Securities strongly believes that 2FA provides better security for its clients and encourages its clients to use 2FA to enjoy an enhanced level of security for online trading.

4. **Can I choose not to use 2FA for trading through KGI Securities?**
   Yes, at this point in time, 2FA is optional and not compulsory for KGI Securities clients. However, should 2FA become mandatory in future, KGI Securities will update its clients accordingly.

5. **What if I choose not to use 2FA for trading through KGI Securities?**
   If you choose not to use 2FA for trading, please note that your confidential data is at risk of being obtained by malicious parties and your computer system may also be exposed to attacks by hackers.

   Nowadays, the increased incidence of direct attacks on online financial systems have caused client's Personal Identification Number (PIN) to become even more vulnerable. Through targeted attacks, client PINs are under constant threats from various types of systems vulnerabilities, security flaws, exploits and scams. Without the use of 2FA, clients may be deceived by hackers into downloading trojans, backdoors, viruses and other malware which cause damage and harmful consequences to them.

6. **How can I protect myself if I choose not to use 2FA for trading through KGI Securities?**
   You should observe the following practices to secure the confidentiality and integrity of your PINs, security tokens, personal details and other confidential data as far as possible. These will help to prevent unauthorised transactions and fraudulent use of your accounts and make sure that no one else would be able to observe or steal your access credentials or other security information to impersonate them or obtain unauthorised access to your online accounts:

You should:

(a) take the following precautions as regards your PIN:

- PIN should be at least 6 digits or 6 alphanumeric characters;
- PIN should not be based on guessable information such as user-id, personal telephone number, birthday or other personal information;
- PIN should be kept confidential and not to be divulged to anyone;
- PIN should be memorised and not to be recorded anywhere;
- PIN should be changed regularly or when there is any suspicion that it has been compromised or impaired; and the same PIN should not be used for different websites, applications or services, particularly when they relate to different entities,

(b) not select the browser option for storing or retaining user name and password;

(c) check the authenticity of our website by comparing the URL and our name in its digital certificate or by observing the indicators provided by an extended validation certificate;

(d) check that the website address changes from 'http://' to 'https://' and a security icon that looks like a lock or key appears when authentication and encryption is expected;

(e) check your account information, balance and transactions frequently and report any discrepancy;

(f) install anti-virus, anti-spyware and firewall software in your personal computers and mobile devices;

(g) update operating systems, anti-virus and firewall products with security patches or newer versions on a regular basis;

(h) remove file and printer sharing in computers, especially when they are connected to the internet;

(i) make regular backup of critical data;

(j) consider the use of encryption technology to protect highly sensitive or confidential information;

(k) log off each and every online session;

(l) clear browser cache after each and every online session;

(m) not install software or run programs of unknown origin;

(n) delete junk or chain emails;

(o) not open email attachments from strangers;

(p) not disclose personal, financial or credit card information to little-known or suspect websites;

(q) not use a computer or a device which cannot be trusted; and

(r) not use public or internet café computers to access online services or perform financial transaction.