山證國際
SHANXI SECURITIES INTERNATIONAL

親愛的客戶：

網絡安全提示

感謝您一直以來對我司的支持。當您使用網絡帶來的便利之際，您亦需小心保護個人賬戶和個人資料的安全。就讓我們為您提供一些有關網絡安全的小貼士吧！

1. 密碼保護

- 在任何情況下，切勿向他人透露您的密碼，山證國際職員也不會索取您的私人密碼作任何用途
- 在設置密碼時，請選擇難以被猜中的組合，密碼的組合應包含字母(大寫及小寫)與數字及最少 8 個位
- 不要使用姓名、出生日期、電話號碼、身份證號碼等部份作為您的密碼
- 定期更換您系統或服務的密碼，建議最少每三個月更改一次
- 不同帳號應設定不同密碼，防止黑客入侵裝置後，以同一組密碼嘗試其他不同的帳號
- 登入系統輸入密碼時，應檢查四周環境是否安全，身旁沒有其他人在窺視您的資料

2. 數據備份

- 數據備份可減少設備損壞及設備遺失的數據損失
- 數據備份應獨立儲存在不同位置及裝置上，可減少裝置丟失或同時損壞的風險
- 使用雲端作數據備份，可減少硬件故障的影響，而且可以在任何地方取回資料
- 數據備份需要持續進行，當設備損壞時可以回復最近一次備份的數據

3. 電腦病毒防護

- 安裝及使用防毒軟件並保持使用最新的病毒定義檔
- 安裝及啟動個人防火牆，可減低黑客入侵電腦的風險
- 請勿下載及安裝來歷不明的軟件，可避免惡意軟件安裝在電腦系統
- 打開來歷不明的檔案前，務必先用保安軟件掃描檔案，可避免被安裝惡意軟件
- 定期為電腦進行掃描以偵測電腦內有否執行惡意軟件

4. 裝置保護及安全

- 請勿使用公用電腦登入重要系統，帳戶資料可能會有被盜的風險
- 請勿使用不知名的 Wi-Fi 熱點，及瀏覽未經加密的網站，個人資訊及帳號會有被盜的風險
- 請勿使用不明途徑電子郵件／即時信息中的連結（包括二維碼）下載山證國際的應用程式或網上服務
- 只通過官方途徑下載應用程式，並留意正確應用程式名稱，以防假冒程式
- 使用 PIN 或密碼鎖上裝置，可以防止任何接觸裝置的人使用
- 確保移動裝置可以追蹤，鎖定或擦除丟失或被盜的設備
- 避免使用系統固件限制破解（越獄版）的手機裝置，破解後的手機裝置會增加安全的風險
- 把裝置系統及應用程式保持最新版本，更新可修補可能存在的保安漏洞
- 在捐獻、出售或回收前，請刪除裝置內的所有資料，可避免裝置內的資料洩漏

山證國際
SHANXI SECURITIES INTERNATIONAL

5. 防釣魚郵件
- 請勿開啟可疑電郵，包括電郵內的連結及附件，打開可疑電郵連結及附件，可被安裝惡意軟件
- 留意寄件者的電子郵件名稱及地址是否正確，可發現電郵是否假冒的
- 對緊急決定的郵件需提高警覺(如密碼即將到期，信用卡付款失敗等)

6. 留意不正常事
- 定期檢查您的賬戶結餘和月結單，如賬戶內有不正常之交易，請立即通知我們
- 定期檢查您的個人資料，以免因被人盜用您的個人資料而造成不必要的損失
- 客戶之通訊資料（流動及聯絡電話號碼）如有任何更改，請盡快通知我們

7. 更多保安資訊

如欲查詢更多有關使用電腦安全的資訊，請參閱以下網站：
- 由政府資訊科技總監辦公室提供「資訊安全網」
  http://www.infosec.gov.hk
- 由政府資訊科技總監辦公室提供「網絡安全資訊站」
  http://www.cybersecurity.hk/tc/index.php
- 由投資者教育中心提供「網上詐騙」
  http://www.thechinfamily.hk/web/tc/scams/scam-websites.html

上述要點會不時更新，請您關注我司以下網站：
http://www.ssif.com.hk/main_hk/customerCenter/cybersecurity/index.shtml

如有垂詢，請聯絡您的客戶經理或致電客戶服務熱線 +852 2501 1001（香港及海外）或 +86 4008411618（中國內地）。

山證國際證券有限公司
山證國際期貨有限公司　　謹啟

2021 年 1 月 8 日