中華民國證券商業同業公會證券商運用人工智慧技術自律規範

金融監督管理委員會 113 年 11 月 19 日金管證券字第 1130361481 號函准予備查
中華民國證券商業同業公會 113 年 11 月 21 日中證商業一字第 1130006063 號公告實施

第一條(目的)

中華民國證券商業同業公會(以下簡稱本公會)為強化證券商運用人工智慧(AI)技術，辦理證券業務的客戶資料保護及風險控管，依據金融監督管理委員會「金融業運用人工智慧(AI)指引」，特訂定本規範。

第二條（名詞定義）

一、 人工智慧 ：係指透過大量資料學習，利用機器學習或相關建立模型之演算法，進行感知、預測、決策、規劃、推理、溝通等模仿人類學習、思考及反應模式之技術。

二、 生成式人工智慧(Generative AI)技術：為人工智慧的一種；係指通過大量資料學習，從而可以生成模擬人類智慧創造之內容的相關技術，其內容形式包括但不限於文本、圖片、聲音、照片、影像、程式碼等。

第三條（原則範圍）

證券商於第一條所載範圍內運用人工智慧，作為與客戶直接互動並提供金融商品建議、或提供客戶服務且影響客戶金融交易權益、或對營運有重大影響者，適用本規範。

本條所指之營運重大影響可參考「證券商作業委託他人處理應注意事項」第四條第五項之重大性定義，自行評估。

第四條（永續發展）

證券商運用人工智慧等技術之策略及執行方向，宜依據國際永續發展目標及自訂之永續發展原則，並適當列入永續發展綜合指標。

第五條（客戶權益）

證券商運用人工智慧技術時，應遵循資通安全、個人資料保護、智慧財產權等金融法規及其他法律規範與相關資訊使用規定。

第六條（公平待客原則）

證券商運用人工智慧時，在演算法設計、開發、資料蒐集、訓練資料選擇、處理及模型建置、生成與優化，及後續應用於金融服務過程中，應採取措施以符合金融服務業公平待客原則。

於處理人工智慧不公正或偏見問題時，以下資料參數得評估是否納入演算法判斷，（如個人屬性資料：姓名、年齡、身心障礙等相關因素），並應就資安、法遵及風控等層面評估風險，依內部程序辦理。

第七條（系統穩健性與安全性）

證券商運用人工智慧技術的模型訓練階段中(包括進行預訓練、優化訓練等)，在選擇模型或演算法等工具時，應注意其安全性與穩定性，並採取有效措施，包含但不限於資料品質處理、模型驗證與監控等，以提高訓練品質防止生成不適當資訊，提升人工智慧技術的輸出或生成內容的準確性與可靠性。

證券商運用人工智慧技術，若涉及金融交易者應理解其如何做出決策並提高模型的可解釋性，以確保對人工智慧的運作之有效管理。

第八條（保護隱私及資訊安全）

證券商運用人工智慧時，處理、儲存、傳輸與使用資料的過程中，應注意保護所有相關個人和組織的資料之隱私權，具備適當的保護措施確保其系統和資料的安全，避免資料洩露，並使用相關安全技術防止、偵測和回應各種安全威脅和攻擊，如駭客攻擊、惡意軟體等。

第九條（建立治理及問責機制）

證券商應指定高階主管或委員會負責人工智慧相關監督管理並建立內部治理架構，並指派單位或人員負責人工智慧之推動及管理，落實辦理人才培育，提供適當之培訓資源。

負責運用生成式人工智慧技術之人員，應掌握該技術的運作方式，以確保回應內容符合背後預測及決策邏輯。

第十條（落實可驗證）

證券商自行開發、優化人工智慧技術時，應保存必要技術文件及相關紀錄，包括開發者在設計、開發和實施過程中，如為可能影響決策的

重要資料、模型或演算法等紀錄，以確保其在必要時可被查驗。

證券商使用第三方人工智慧技術時應執行調查、評估及監督作業，以確保第三方業者在人工智慧運算有留存軌跡紀錄，俾利後續查驗。

證券商導入第三方人工智慧技術時，宜要求提供相關資訊，並明訂責任範疇。

第十一條（落實透明性）

證券商運用人工智慧技術與客戶直接互動時，應告知該互動或服務係利用人工智慧技術自動完成，或揭露該互動或金融服務其適用之人群、場景或用途。另宜由客戶自行選擇是否使用，並提醒客戶該項服務有無替代方案，但法規另有其他規定者，從其規定。

第十二條 (內部管理架構)

證券商提供前條金融服務前，應針對所使用資料之治理方式、資通安全、監督機制、客戶權益保障及發生非預期事件時之應變措施等進行評估，並由資安、法遵及風控等單位或人員對於上開內容提出意見。

第十三條（風險管理機制）

證券商應以風險基礎為導向，視其營業規模及運用人工智慧技術之程度建立適當之風險管理及定期檢視機制，視相關風險大小/特性/範圍，得由具人工智慧專業之獨立第三人出具評估報告，評估的內容應包括資料品質、模型品質、系統安全性，以及公平性、永續發展、透明性及可解釋性等，並且根據評估結果調整和改進相關的策略和措施。

外國證券商在臺分(子)公司，其風險管理、定期檢視機制及評估報告得由外國總(母)公司出具。

證券商運用生成式人工智慧，對於其產出之資訊，仍需由證券商就其風險進行評估與管控。

第十四條（第三方業者委外管理）

證券商對於涉及營業執照所載業務項目或客戶資訊之相關人工智慧作業委外時，應依據「證券商作業委託他人處理應注意事項」規定辦理。

第十五條 （內部控制制度）

證券商應將本自律規範內容，納入內部控制制度，並定期辦理查核。

第十六條 （施行程序）

本自律規範經本公會理事會會議通過，並報奉主管機關備查後實施，修正時亦同。