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

條文	說明
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。	參考金管會 113 年 6 月 20 日公告「金融業運用人工智慧(AI)指引」(以下簡稱 AI 指引)，及銀行公會 113 年 5 月 6 日公告「金融機構運用人工智慧技術作業規範」訂定。
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。	參考 AI 指引「總則章」-共通事項，有關人工智慧(AI)相關定義訂定。
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。	一、參考 AI 指引「總則章」-共通事項第三點風險評估考量因素，證券商運用 AI 之風險評估須考量是否面對客戶、使用個人資料的程度、AI 在決策中使用的程度、AI 系統的複雜性、影響不同利害關係人的程度及廣度及是否提供救濟選項。 二、參考銀行業做法：所謂直接互動，係指人工智慧技術透過分析提問內容及前後文關係，掌握提問目的，產生非預期回應訊息，且互動過程中無人介入。(例如：

條文	說明
	客戶透過與證券商之聊天機器人或語音助理進行多回合的人機互動。) 三、本自律規範所稱之重大性，係指證券商遭遇下列情形，例如：人工智慧無法提供服務或有資訊安全疑慮、涉及客戶資料安全事件，對證券商營運或客戶權益有重大影響等事件。
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。	參考AI指引第六章「促進永續發展」，證券商運用人工智慧(AI)技術以促進永續發展為原則。例如：證券商運用人工智慧，不僅可以提高內部流程的效率，還可以降低能源消耗和營運成本，從而促進永續發展。
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。	參考 AI 指引第三章「保護隱私及客戶權益」，證券商運用人工智慧(AI)技術應保護客戶隱私，妥善管理及運用相關資訊，避免導致個人資料外洩之風險。
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。	參考 AI 指引第二章「重視公平性及以人為本的價值觀」，證券商在應用 AI 系統時，必須充分認知並儘可能避免潛在的演算法偏見，尤其對於面對客戶所提出之 AI 服務，必須確認資料來源的合宜性及數據資料之品質，在正式推出前於獨立環境中測試及驗證演算法，以避免產出市場不樂見之結果，儘可能讓每個客戶都能獲得公平、非歧視性的金融服務，以實現普惠金融之目標。
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	一、 參考AI指引第四章「系統穩健性與安全性」，證券商在運用 AI 模型訓練時，系統之穩健及安全對金融機構之正常運作即愈

條文	說明
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。	顯重要，因此選擇具韌性的 AI 模型，蒐集資料時宜注重資料品質，視情況對模型進行交互驗證及對抗性測試，建立資安防護措施，防範各種安全威脅及攻擊，並進行持續監控，以確保 AI 系統的整體安全與穩定運行。明訂證券商對資訊作業之災害應變相關作業流程。 二、 參考 AI 指引第五章「落實透明性與可解釋性」，所稱可解釋性，係指可清楚說明自行或委託研發並使用之 AI 系統如何運作及其預測或決策過程背後之邏輯，以利組織內評估是否符合內部政策、作業流程及監管要求等。
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。	參考 AI 指引第三章「保護隱私及客戶權益」，證券商為使人工智慧達成準確性目的，可能需要蒐集消費者或客戶大量資訊，因此要特別注意保護客戶的隱私權，建立適當之資安防護或管控措施，妥善處理其客戶資料，避免資料外洩風險。
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。	一、參考 AI 指引第一章「建立治理及問責機制」，證券商應對其使用之人工智慧承擔相應之內、外部責任。內部責任包含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；外部責任則涉及對消費者與社會之責任，包括保護消費者之隱私及資訊安全等。 二、參考 AI 指引第五章「落實透明性與可解釋性」係證券商在自行或委託研發並使用之 AI 系統如何運作及

條文	說明
	其預測或決策過程背後之邏輯，以利組織內評估。
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。	一、 參考 AI 指引第五章「落實透明性與可解釋性」，證券商在人工智慧「系統規劃及設計」階段中，對於自行研發之人工智慧，宜規劃備置人工智慧架構相關文件，並規劃確認提供主管機關存取及使用權限，以便未來其查詢與瞭解證券商人工智慧之運作及使用數據之妥適性。 二、 若運用第三方業者開發或營運之人工智慧提供金融服務，應對第三方業者進行適當之風險管理及監督。
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。	參考 AI 指引第五章「落實透明性與可解釋性」，證券商運用人工智慧提供客戶商品或服務時應向消費者適當揭露與其相關之資訊。
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。	參考 AI 指引第一章「建立治理及問責機制」，證券業用人工智慧要有明確的管理架構及風險管理政策，且對內要能夠解釋清楚系統的運作邏輯、對外要能說明整體政策、客戶對人工智慧需知悉之事項等，並應有完整之處理錯誤或非預期事件之程序。
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	一、 參考 AI 指引第一章「建治治裡及問責機制」，證券商應建立人工智慧風險管理機制，並整合至現行風險管理及內部控制作業或流程中，且應進行定期的評估及測試。

條文	說明
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。	二、 證券商運用人工智慧之風險高低仍由業者綜合考量各風險評估因素後自行判斷，可參考 AI 指引內容，以下所舉其中例子： 提供客戶服務(面對客戶)之人工智慧，決策結果對客戶權益或營運有重大影響之 AI 系統，通常有較高之風險性，例如用於信用評分、機器人理財等；AI 決策結果僅係提升客戶服務品質者之 AI 系統，風險性可能較低，例如智能客服。
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。	參考 AI 指引「總則章-共通事項」，證券商委託第三方業者導入人工智慧應符合「證券商作業委託他人處理應注意事項」規範。
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。	參考 AI 指引「第一章-建立治理及問責機制」，證券商可將 AI 風險管理整合至現有的風險管理及內部控制架構，整合項目包括模型風險管理、資訊安全、資料保護及公平待客等現有既有架構，如尚有不足，可再增訂納入風險管理及內部控制架構以符合 AI 核心原則。
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。	