客戶個人資料保護及資訊系統安全防護辦法

最新修訂日期：2025/06/16

第一條 規範目的

一、 萃科科技股份有限公司（下稱本公司）預計保存客戶資訊及法定應保存之文件、檔案及資訊，並透過將電磁紀錄及紙本文件截圖、下載、匯出、拍照、掃描或其他方式轉換為可儲存於資訊系統之電子檔案，將之保存於網路附接儲存裝置（下稱 NAS）或第三方網路服務商提供之雲端儲存空間（下稱雲端）。

二、 為規範客戶資訊、法定應保存之文件、檔案及資訊之蒐集、處理及利用，保護客戶之個人資料及隱私權，並維護資訊系統之安全，本公司爰依《個人資料保護法》及《金融監督管理委員會管理虛擬資產平台及交易業務事業（VASP）指導原則》等相關法規，制定《客戶個人資料保護及資訊系統安全防護辦法》（以下簡稱「本辦法」）。

第二條 名詞解釋

一、客戶資訊：指本公司於交易前及交易過程中提供客戶簽署及填寫之文件等，及為執行確認及驗證客戶身分程序（KYC）加強式客戶盡職調查程序（EDD）等作業流程，而蒐集或要求客戶提供若干個人資料並製作之相關文件，包括但不限於下列資料及文件：

(一) 執行確認客戶身分程序（KYC）時取得之客戶個人資料。

(二) 執行高風險客戶加強式盡職調查程序（EDD）取得之客戶個人資料。

(三) 交易紀錄及交易憑證。

(四) 客戶之風險評級分數。

(五) 以客戶之個人資料進一步於第三方資料庫或使用幣流分析軟體與區塊鏈瀏覽器搜尋所取得之資訊。

二、法定應保存之文件、檔案及資訊：指依據《提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法》及《金融監督管理委員會管理虛擬資產平台及交易業務事業（VASP）指導原則》等相關法令規定，本公司與客戶建立業務關係及交易時應保存之文件、檔案及資訊。

三、資訊系統：指 NAS、雲端或其他可供儲存客戶資訊、法定應保存之文件、檔案及資訊之資訊系統。

四、電子檔案：指資訊系統所顯示之電磁紀錄。

五、管理權限人員：指本公司徵審單位主管、風險控制單位主管與技術單位主管。技術單位主管具有本公司資訊系統之管理權限；徵審單位主管負責保管紙本文件之櫃位或抽屜之鑰匙。

第三條 權責單位

本公司就客戶個人資料保護及資訊系統安全維護業務應由技術單位、徵審單位以及風險控制單位負責統籌辦理，且由法遵單位進行政策與辦法之制定，並應配置相當資源，其任務如下：

一、確保客戶資訊及法定應保存之文件、檔案及資訊之電子檔案有妥適存放於資訊系統，紙本文件則應妥適存放於附加鑰匙鎖之櫃位或抽屜，且應確保所有資料之隱密性、安全性及正確性，並應由管理權限人員負責控管客戶資訊及法定應保存之文件、檔案及資訊之存取及調用。

二、應為資訊系統設置適當之防護機制，例如開啟防火牆、使用防毒軟體、委託第三方服務提供防止外部網路入侵之解決方案或服務等。
三、應確保資訊系統具有監控機制，得以記錄使用者存取之軌跡紀錄，並得以監控異常非法或異常使用行為。
四、規劃、訂定、修正與執行本辦法及業務終止後客戶個人資料處理等相關事項。
五、訂定個人資料保護管理政策，將本公司蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項，公告使本公司人員明確瞭解，且應使客戶知悉及取得客戶同意，並擬定、修正及管理本公司提供給客戶簽署之《個人資料提供同意書》。
六、定期對本公司人員施以基礎認知宣導或專業教育訓練，使其明瞭資訊系統安全防護相關管理措施、個人資料保護相關法令規定、責任範圍及各種客戶個人資料保護之方法或管理措施。
七、定期就各項任務之執行任務情形向本公司董事（會）報告。

第四條　客戶資訊保存基本原則

保存客戶資訊及法定應保存之文件、檔案及資訊時，本公司應遵循以下基本原則：
一、任何儲存、處理中及編輯中之資料均應保護，如機密之資訊（包括電子檔案或紙本）應有適當之保護，以維護其機密性並防止非法存取；同時應保留各項存取之軌跡紀錄，以確認重要活動之詳細資料，並僅授權予適當人員存取。
二、任何透過資訊系統儲存、處理中及編輯中之資料（包括客戶資訊及法定應保存之文件、檔案及資訊）均應保護，以防不當竄改、操縱或破壞毀損。如屬重要資訊，應有適當之保護，以防非法更動。
三、確保資訊系統及文件保管機制持續運作，當合法使用者要求使用或主管機關調閱時，均可在適當之時間內獲得回應。

第五條　個人資料之蒐集、處理及利用

一、各單位應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。
二、各單位對於個人資料之蒐集、處理或利用，應確實依個資法第五條規定為之，遇有疑義者，應提請法遵單位研議。
三、依個資法第六條第一項但書規定蒐集、處理或利用有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，應報請法遵單位同意後為之。
四、各單位蒐集當事人個人資料時，應明確告知當事人下列事項；但符合個資法第八條第二項規定情形之一者，不在此限：
(一) 本公司名稱。
(二) 蒐集之目的。
(三) 個人資料之類別。
(四) 個人資料利用之期間、地區、對象及方式。
(五) 當事人依個資法第三條規定得行使之權利及方式。
(六) 當事人得自由選擇提供個人資料時，不提供將不提供將對其權益之影響。
五、各單位蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及個資法第八條第一項第一款至第五款所列事項；但符合個資法第九條第二項規定情形之一者，不在此限。
六、前條之告知義務，得於首次對當事人為利用時併同為之。
七、第一項非由當事人提供之個人資料，於個資法修正施行前即已蒐集者，除有個資法

第九條第二項所訂免為告知之情形外，應依個資法規定進行告知。

八、各單位依個資法第十九條第五款及第二十條但書第六款規定經當事人書面同意者，應取得當事人同意書。

九、各單位依個資法第十九條或第二十條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。各單位依個資法第十九條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。對於個人資料之利用，不得為資料庫之恣意連結，且不得濫用。

十、本公司保有之用戶資料有誤或缺漏時，應由資料蒐集單位簽奉核定後，移由風險控制單位更正或補充之，並留存相關紀錄。

十一、 本公司保有之個人資料正確性有爭議者，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料；但符合個資法第十一條第二項但書情形者，不在此限。個人資料已停止處理或利用者，風險控制單位應確實記錄。

十二、 本公司保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位簽奉核定後，移由風險控制單位刪除並停止處理或利用；但符合個資法第十一條第三項但書情形者，不在此限；個人資料已刪除、停止處理或利用者，風險控制單位應確實記錄。

十三、 各單位依個資法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐集、處理或利用個人資料者，應簽奉核定後移由風險控制單位為之；個人資料已刪除、停止蒐集、處理或利用者，資料保有單位應確實記錄。

十四、 各單位遇有個資法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，須依通報程序進行通報，經查明後，應由法遵單位依本公司相關訊息發布程序進行訊息之發布並以適當方式儘速通知當事人。

第六條　當事人行使權利之處理

一、 當事人依個資法第十條或第十一條第一項至第四項規定向本公司為請求時，應填具個人資料申請單，並檢附相關證明文件。

前款書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，應以書面駁回其申請：

(一) 申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正者。

(二) 有個資法第十條但書各款情形之一者。

(三) 有個資法第十一條第二項但書或第三項但書所定情形之一者。

(四) 與法令規定不符者。

二、 當事人依個資法第十條及第十一條規定提出之請求之准駁、延長，應依個資法第十三條規定期間內辦理，並應將其原因以書面通知請求人。

三、 當事人閱覽其個人資料，應依本公司相關檔案文件調閱程序辦理。

第七條　個人資料保護及資訊系統安全防護管理措施

一、本公司應將客戶資訊及法定應保存之文件、檔案及資訊之電子檔案存放於資訊系統，紙本文件則應妥適存放於附加鑰匙鎖之櫃位或抽屜，且應確保所有資料之隱密性、安全性及正確性，並應由管理權限人員負責控管客戶資訊及法定應保存之文件、檔案及資訊之存取及調用。

二、本公司為維護所保有之客戶資訊及法定應保存之文件、檔案及資訊之安全，應採取下列保護管理措施：

(一) 訂定各類設備或資訊系統之使用規範，及報廢或轉作他用時應採取防範資料洩漏之適

當措施。

(二) 針對所保有之客戶個人資料內容有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

(三) 作業過程有備份客戶個人資料之需要時，對備份資料予以適當保護。

(四) 訂定紙本資料之銷毀程序。

(五) 電腦或資訊系統需報廢汰換或轉作其他用途時，應採取適當防範措施避免洩漏個人資料。

三、本公司以資訊系統儲存客戶資訊及法定應保存之文件、檔案及資訊之電子檔案時，或利用資訊系統蒐集、處理或利用客戶個人資料時，應採取下列資訊系統安全防護管理措施：

(一) 使用者身分確認及保護機制。

(二) 客戶個人資料顯示之隱碼機制。

(三) 網際網路傳輸之安全加密機制。

(四) 資訊系統於開發、上線、維護等各階段軟體驗證及確認程序。

(五) 資訊系統之存取控制及保護監控措施。

(六) 防止外部網路入侵對策。

(七) 非法或異常使用行為之監控及因應機制。

第八條 作業流程

一、本公司於客戶註冊交易時，應為客戶編號及建立該客戶之NAS資料夾、雲端資料夾或其他資訊系統之資料夾（如有需要），並確保客戶每次交易之紀錄皆完整保留於交易系統，若有紙本文件，亦應於兩個工作日內存放至保存之櫃位或抽屜。

二、文件、檔案、資訊之建檔：

(一) 徵審單位與風險控制單位應將客戶之各項紙本資料及文件編碼，並應裝訂以便留存。

(二) 文件、檔案、資訊之電子檔案檔名編碼方式以客戶編號+各類別文件、檔案、資訊（編號）。同一項文件若有多個檔案，應按順序予以編碼，以利識讀。

(三) 徵審單位人員確認客戶之各項文件、檔案、資訊電子檔案已成功傳送至本公司NAS資料夾、雲端資料夾或其他資訊系統之資料夾後，應將客戶之各項文件、檔案、資訊電磁紀錄於當日自個人使用設備中刪除。

三、文件、檔案、資訊之保存/存取

(一) 紙本文件：

應置放於風險控制單位附加鑰匙鎖之櫃位或抽屜，且鑰匙應由管理權限人員負責保管。有存放或取用文件需求之人員應向管理權限人員提出申請，取得管理權限人員核准後，始得存放或取用文件。

(二) 電子檔案：

應存放於資訊系統，且存放或取用皆應取得管理權限人員之同意。資訊系統應記錄存取之軌跡，包含何人、何時存取。本公司人員離座或下班時須啟動電腦螢幕保護裝置，或將個人使用設備關機，或將帳號登出。

四、個人資料保存之資訊安全控管

(一) 本公司將使用資訊系統保存客戶資訊及法定應保存之文件、檔案及資訊之電子檔案。具有資訊系統管理權限者為本公司技術單位主管。

(二) 前款管理權限人員對於登入資訊系統應使用高強度密碼，且應定期更換密碼，並

宜採取雙重驗證機制（又稱為兩步驟驗證，即2FA）管控，以確保資訊安全及客戶個人資料之隱私安全。

(三) 本公司各項紙本文件、檔案、資訊紀錄存放之櫃位或抽屜平時均應上鎖，具有開啟櫃位或抽屜鑰匙之持有者即具備管理權限者為本公司風險控制單位主管。

五、文件、檔案、資訊之調閱/傳送

(一) 紙本文件

1. 徵審單位人員、風險控制單位人員或公司其他人員若有調閱客戶紙本文件、檔案、資訊紀錄需求時，應取得管理權限人員以及法遵單位最高主管之同意，並應妥善記錄調閱者、調閱之特定文件、檔案、資訊、調閱之目的與使用及歸還時間；管理權限人員於核准前，應詢問該名人員存取文件、檔案、資訊之目的，核可後並應要求該名人員確實登記其姓名、存取之時間、存取之文件、檔案、資訊名稱，且應嚴格要求該名人員不得擅自取用或瀏覽非本次核准之文件、檔案、資訊。管理權限人員離座或下班時，應妥善確保鑰匙非其他人所能取得。
2. 如需傳送客戶紙本文件、檔案、資訊紀錄至公司外部，應取得管理權限人員之同意，並告知傳送至外部之原因、目的及收受者，且須妥善封存後以掛號或快遞方式寄出以留存傳送軌跡。

(二) 電子檔案

1. 徵審單位人員、風險控制單位人員或公司其他人員若有調閱客戶文件、檔案、資訊紀錄之電子檔案需求，應取得管理權限人員以及法遵單位最高主管之同意，並採取最小權限原則，由管理權限人員單獨授予調閱者開啟資訊系統中特定文件、檔案、資訊之權限，並應妥善記錄調閱者、調閱之特定文件、檔案、資訊、調閱之目的與開放、關閉權限之時間。
2. 如需傳送客戶文件、檔案、資訊紀錄之電子檔案至公司外部，需檢附相關文件（包括但不限於公文書），並應取得管理權限人員以及法遵部門最高主管之同意，並告知傳送至外部之原因、目的及收受者，與外部單位協調達成共識，使用加密電子郵件始得傳輸。

第九條　資料銷毀

一、本公司於交易前及交易過程中蒐集客戶資訊、法定應保存之文件、檔案及資訊之紙本及電子檔案應至少保存至交易結束後五年。但法令另有較長保存期間規定者，從其規定。

二、前項所示客戶資訊、法定應保存之文件、檔案及資訊正受司法機關、檢察機關、司法警察或主管機關調查或刻正進行訴訟程序，各文件、檔案及資訊之紙本、電子檔案均應留待法院判決定讞、檢察官不起訴處分確定或行政機關完成調查，且同時屆滿前項所示期限後，始得銷毀之。

三、資料之銷毀，非經取得法遵單位之核准，不得為之。

四、資料銷毀之相關規定，詳參《文件銷毀程序辦法》。