現觀科技股份有限公司

個人資料保護管理辦法

110 年 12 月 9 日訂定

第一條　制定目的

為確保本公司各項業務之執行符合個人資料保護法(「個資法」)、歐盟「一般資料保護規則」(General Data Protection Regulation, "GDPR")相關法規或法令之要求及釐清員工應遵循的個人資料保護目標，於合理的範圍內蒐集、處理及利用個人資料，建立本公司執行業務或管理內部人員，對於客戶及員工個人資料使用的依據，降低本公司與員工可能的法律風險，保障客戶權益及維護本公司信譽。

第二條　適用對象與範圍

一、適用對象：本公司及子公司所有人員、與本公司有業務往來之廠商或顧問（包含其員工或臨時雇員），均屬之。

二、範圍：本辦法保護對象為個資法所保護之個人資料。針對蒐集、處理、利用及國際傳輸個人資料訂定相關規範，確保個人資料之安全。

第三條　名詞定義

名詞定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、間接方式識別：指資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

三、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
四、蒐集：指以任何方式取得個人資料。
五、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
六、刪除：指使已儲存之個人資料自個人資料檔案中消失。
七、利用：指將蒐集之個人資料為處理以外之使用。
八、國際傳輸：指將個人資料作跨國（境）之處理或利用。
九、公務機關：指依法行使公權力之中央或地方機關或行政法人。
十、當事人：指個人資料之本人。
十一、個人：指現生存之自然人。

第四條　當事人權利

當事人就其個人資料行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。
二、請求製給複製本。
三、請求補充或更正。
四、請求停止蒐集、處理或利用。
五、請求刪除。

第五條　委託蒐集

一、委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。
二、第一項之監督，應定期確認受託者執行之狀況，並將確認結果記錄之。
三、受託者僅得於本公司指示之範圍內，蒐集、處理或利用個人資料。受託者認本公司之指示有違反個資法、GDPR、其他個人資料保護法律或其法規命令者，應立即通知本公司。

第六條　個資蒐集最小化

本公司對於個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得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。

第七條　不得蒐集內容

本公司對於有關個人病歷、醫療、基因、性生活、健康檢查及犯罪前科之資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。
二、履行法定義務所必要，且有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、為協助公務機關執行法定職務或為本公司履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
五、經當事人書面同意。但逾越特定目地之必要範圍或其他法令另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，仍不得蒐集之。

第八條　書面同意

所稱書面同意，指當事人經本公司明確告知利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。

第九條　告知義務

一、本公司向當事人蒐集個人資料時，應明確告知當事人下列事項：

1. 本公司之名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依第四條規定得行使之權利及方式。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

二、有下列情形之一者，得免為前項之告知：

1. 依法律規定得免告知。
2. 個人資料之蒐集係履行法定義務所必要。
3. 告知將妨害公務機關執行法定職務。
4. 告知將妨害公共利益。
5. 當事人明知應告知之內容。
6. 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第十條　非當事人提供之個資

一、本公司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所應告知事項。

二、有下列情形之一者，得免為前項之告知：

1. 有前條第二項所列各款免為告知之情形。
2. 當事人自行公開或其他已合法公開之個人資料。
3. 不能向當事人或其法定代理人為告知。
4. 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

第十一條　資料答覆

本公司依當事人之請求，應就蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
二、妨害公務機關執行法定職務。
三、妨害本公司或第三人之重大利益。

第十二條　義務

一、本公司應維護個人資料之正確，並應主動或依當事人之請求更正或

補充之。

二、個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

三、個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

四、當事人認為有違反本辦法規定蒐集、處理或利用個人資料者，本公司應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

五、因可歸責於本公司之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第十三條　個資外洩通報程序

一、如發生個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

二、知悉前項之侵害時起 72 小時內，應由專責單位通報資料保護主管機關。但個資侵害不會對自然人之權利和自由造成風險者，不在此限。倘未能於 72 小時內通報監管機關者，應敘明遲延之理由。

第十四條　資料之抄錄

一、當事人對於其個人資料，得請求本公司答覆查詢、提供閱覽或製給複製本。受理單位應於十五日內回復請求；必要時得延長十五日，並應將其原因以書面通知請求人。

二、本公司對於查詢或請求閱覽個人資料或製給複製本者，受理單位得酌收必要成本費用。

第十五條　資料之刪除

一、當事人對於其個人資料，得請求本公司刪除、停止蒐集、處理或利用其個人資料。

二、受理單位對於前項請求之決定，應敘明處理方式及理由，以簽呈或其

他適當方式，經專責單位核准後於三十日內回復當事人。

三、前項處理，應將相關文件及處理情形，歸檔保管之。

第十六條　蒐集及處理

一、本公司對個人資料之蒐集或處理，應有特定目的，並符合下列情形之一者：

1. 法律明文規定。
2. 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 經當事人書面同意。
5. 增進公共利益所必要。
6. 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
7. 對當事人權益無侵害。

二、蒐集或處理者知悉或經當事人通知，依前項第六款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第十七條　個資之利用

本公司對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、經當事人書面同意。

六、有利於當事人權益。

第十八條　跨境傳輸

本公司國際傳輸個人資料，而有下列情形之一者，應為禁止之：

一、涉及國家重大利益。
二、國際條約或協定有特別規定。
三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
四、以迂迴方法向第三國（地區）傳輸個人資料規避相關法令。

第十九條　業務檢查

一、本公司各單位人員應配合中央目的事業主管機關或直轄市、縣（市）政府，為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查。
二、參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

第二十條　行政救濟

本公司各單位對於任何行政機關、或他國政府單位之要求、強制、扣留或複製行為不服者，應即通知本公司專責單位，提起聲明異議或行政訴訟救濟，以維護本公司權益。

第二十一條　安全措施

本公司保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第二十二條　資訊安全

一、本公司為防止個人資料被竊取、竄改、毀損、滅失或洩漏，應採取技術上及組織上之適當安全維護措施。
二、前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

1. 配置管理之人員及相當資源。
2. 界定個人資料之範圍。
3. 個人資料之風險評估及管理機制。
4. 事故之預防、通報及應變機制。
5. 個人資料蒐集、處理及利用之內部管理程序。
6. 資料安全管理及人員管理。
7. 認知宣導及教育訓練。
8. 設備安全管理。
9. 資料安全稽核機制。
10. 使用紀錄、軌跡資料及證據保存。
11. 個人資料安全維護之整體持續改善。

第二十三條　專責單位

一、本公司成立「個人資料保護管理執行小組」由本公司主管及專人共同組成，任務如下：

1. 本公司個人資料保護政策之擬議。
2. 本公司個人資料管理制度之推展。
3. 本公司個人資料風險之評估及管理。
4. 本公司職員工之個人資料保護意識提升及教育訓練計畫之擬議
5. 本公司個人資料管理制度基礎設施之評估。
6. 本公司資料管理制度適法性與合宜性之檢視、審議及評估。
7. 其他個人資料保護、管理之規劃事項。

二、為遵循 GDPR 相關規範，本公司得設置歐盟代表（EU Representative）及資料保護官（Data Protection Officer, DPO）。

三、為遵循 GDPR 相關規範，必要時應執行資料保護影響評估（Data Protection Impact Assessment, “DPIA”）。

第二十四條　相關法令

一、利害關係人對於本辦法有任何疑議與建議者，皆可以書面資料向人資單位建議討論。

二、本辦法依相關之中央目的事業主管機關所訂定個人資料檔案安全維護計畫，同步調整內容與更新，於本公司公告。如有與主管機關法令衝突之處，皆依主管機關法令為準。

第二十五條　相關文件

一、員工基本資料表暨個資同意書

二、資料保護影響評估表（Data Protection Impact Assessment, “DPIA”）

第二十六條　核准及修正

本辦法呈請董事會核准後公告施行之，修改時亦同。