昕奇雲端科技股份有限公
個人資料保護管理辦法

第 一 條 目的

本公司為落實個人資料之保護與管理，依台灣行政院公布之「個人資料保護法」（以下簡稱個資法）特訂定本管理辦法。

本辦法不足部份依個人資料保護法及個人資料保護法施行細則辦理。

第 二 條 範圍

本辦法適用於本公司全體在職員工(含臨時工、顧問)、離職員工及應徵本公司職務人員。

第 三 條 定義

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、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。(包含備份檔案)

三、蒐集：指以任何方式取得個人資料。

四、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。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、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。

八、 非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

十、資料管理單位(或稱權責單位)：為所屬業務與因業務執行而進行資料蒐集、處理、利用資料之業務執行單位。

十一、各單位：指本公司各行政及業務相關單位。

第 四 條 作業程序

一、 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：

(一)、法律明文規定。

(二)、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。

(三)、當事人自行公開或其他已合法公開之個人資料。

(四)、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

(五)、經當事人書面同意。

(六)、為增進公共利益所必要。

(七)、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。

(八)、對當事人權益無侵害。 蒐集或處理者知悉或經當事人通知依前項第七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。

(九)、本公司若有必要公布個人資料時，需經核准並遵循相關法令規範。

二、 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。

三、 當事人就其個人資料依本法規定行使之下列權利，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。

四、 向當事人蒐集個人資料時，應明確告知當事人下列事項：

(一)、機關或單位名稱。

(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)、當事人依前項之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，不提供將對其權益之影響。五、 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。

五、 本公司保有之個人資料有誤或缺漏時，應由資料管理單位經當事人同意後，更正或補充之，並留存相關紀錄。

六、 當事人提出之請求之准駁、延長，應依個資法規定期間內辦理，並應將其原因以書面通知請求人。但因本公司執行職務或業務所必需者及受其他法律所規範者，本公司得拒絕之。

七、 各單位依當事人之請求刪除、停止蒐集、處理或利用個人資料者，應經簽核後為之。

八、 個人資料已刪除、停止蒐集、處理或利用者，資料管理單位於文件備註欄位內應確實記錄。

九、 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；存取個人資料時應視需要考量設置權限、加密機制，並留存相關紀錄及個資使用者身份以供事後查對。

十、 經授權存取個人資料檔案之使用者帳號必須管控，不應共用帳號；個人資料處理人員應克盡保密之責，並於職務有異動或離職時，取消停用其使用者帳號。

十一、 經授權傳輸個人資料時需加密與留存紀錄，紙本文件需彌封安全的方式傳遞。

十二、 含有個人資料紙本文件不再使用時，應以碎裂方式進行破壞使其無法閱讀識別，並刪除電子檔，嚴禁回收使用。

十三、 設備管理：

(一)、應指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。

(二)、儲存個人資料之資訊設備須置放於實體安全區域（如：門禁控管之辦公區域、機房）。

(三)、儲存個人資料檔案之儲存媒體，須建立備援機制。

(四)、儲存個人資料檔案之媒體須有攜出、拷貝或複製的管控機制，並留存紀錄。

(五)、外部廠商或個人更新或維修儲存個人資料檔案之電腦設備時，單位須指派專人在場確保資料安全。

(六)、儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，須刪除其所儲存之個人資料檔案。

十四、 個資事故通報及回應機制：

個人資料保有單位於個資法第十二條所定個人資料有被竊取、洩漏、竄改或其他侵害情事者，應先行通報並進行緊急因應措施，其作業程序如下：

(一)、個人或單位接獲個人資料安全事件通知。

(二)、個人或單位主動先行通報。

(三)、個資委員會釐清資料保有、處理等作業程序與責任所屬。

(四)、資料權責單位應即進行防禦或補救作業。

(五)、資料權責單位應即以適當方式通知當事人。

(六)、資料權責單位應將改善與預防措施納入工作準則，以降低事件再發生機率。

(七)、回報執行小組。

十五、 本公司制定個資保護與資訊安全管理政策，並且建立個資事故對財務報表影評估機制，進行關鍵個資系統及隱私衝擊分析。

十六、 若有重大個資事故，應評估對財務報表是否發生重大影響，並依主管機關指示、或相關會計處理原則及法規辦理之。

十七、 其他

(一)、公司建置個資之專責組織，依職能適當分工。

(二)、公司不定期實施個資保護教育訓練及宣導，以提高相關人對個資保護之認知。

(三)、公司需定期針對個人資料進行盤點。

(四)、公司需設置個人資料之蒐集、處理及利用之程序。

(五)、稽核單位不定期查核個資管理政策之實施。

第 五 條 實施及修訂

本管理辦法經董事會通過後實施，修訂時亦同。

本辦法於西元 2020 年 12 月 25 日制訂。

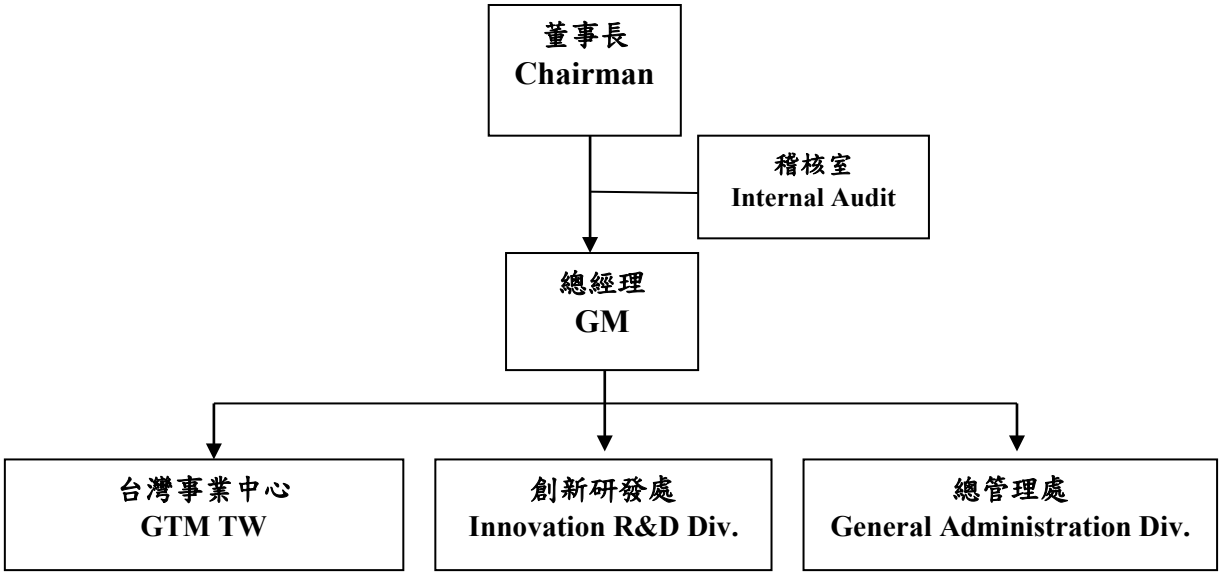
本辦法於西元 2023 年 03 月 17 日第一次修訂。

第 六 條 附件

附表一：個人資料保護委員會組織圖

附表一

個人資料保護委員會組織圖

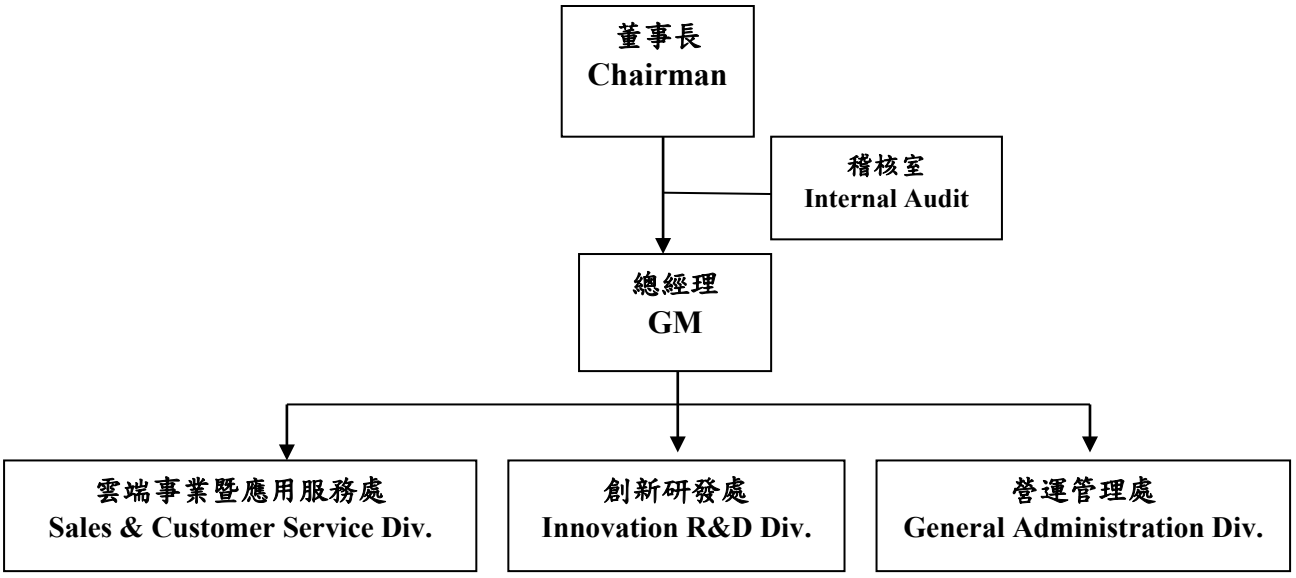


附表二

事故通報流程

附表一(作廢)

個人資料保護委員會組織圖



(以下未列正式辦法)

第 七 條 通報及應變程序

一、個資安全事故之通報程序

（一）於獲悉個資當事人抱怨、間接獲知個資因竊取、竄改、毀 損、滅失、洩漏或其他侵害等，或是發現個資安全事故已 發生或可能發生，應立即檢視事件重大性並於當日通報個 人資料保護管理委員會（以下簡稱「個資委員會」）。

（二）倘事件具有緊急重大性，且涉及資訊設備之緊急修復時，同仁應於通報個資委員會後，迅速協助知會相關處理單位（例如：資圖處），進行處理。

（三）同仁於通報後，應即將通報內容及初步處理狀況記錄於「個資安全事故紀錄單」中，並送單位主管簽核後，由個資委員會保存。

二、個資安全事故之緊急處理程序

（一）個資委員會收到通報後，若認該事件將使個資可能在短時 間內遭到毀損、滅失、洩漏或其他侵害時，或如不進行緊 急處理可能使得損害快速擴大時，應即通知相關人員或協力廠商進行緊急處理。

（二）緊急處理措施

1. 應以業管單位為原則，惟個資委員會視情況需要，得進行必要之指揮監督。
2. 緊急處理時，應採取免於個資繼續受到毀損、滅失、洩漏之保護措施，例如於災難現場快速打包個資，並進行清點。

（三）緊急處理後，個資委員會應根據事故狀況進行調查、通報個資當事人、維護個資正確性、更正錯誤、改善整體環境或通報主管機關等作業。

（四）緊急處理後，個資委員會應將處理情形填載於「個資安全 事故紀錄單」。

（五）關於事件發生後之個資正確性維護、錯誤之更正或整體環 境之改善，由個資委員會責成相關單位進行後續處理。相關單位於後續處理完成後，應於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。

（六）如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知個資當事人及取得其書面同意。

三、個資安全事故處理程序

（一）於事故初步處理完畢後，個資委員會應依下列方式，查明事故發生之原因：

1. 內部調查

(1) 資訊單位：清查可能導致事故發生或資料外洩之缺口，透過檢視相關Log紀錄，如電子郵件傳送紀錄、資料下載紀錄等，分析可能導致事務之人員、時間及方式。

(2) 稽核單位：清查事故發生相關之作業程序，透過作業流程檢視、文

件檢視、單位主管覆核紀錄等，以指出可能之問題所在。

(3) 各單位主管：檢視其單位之相關書面文件是否遭竊、非授權複製、拷貝等情況。

2. 外部調查

(1) 得委託外部顧問本校進行鑑識稽核作業，透過特定 檢視程序，對引起事故發生之可能處進行流程查訪，以確認問題之所在。

(2) 得委託徵信單位，對於本校內部可能導致事故之特定人員或外部有心人士進行可能犯罪行為進行收集、監視，並提供本校蒐集、分析之結果。

(3) 詢問個資當事人得知受害之相關情形和管道，並據 以了解事件發生原因。

(4) 詢問導致事故發生之本校內、外部人員及其曾接觸之人員。

(二) 查明事故發生原因後，個資委員會應填寫「個資安全事故通知當事人紀錄單」，並依照個人資料保護法第 12 條所要求，透過適當方式通知個資當事人，通知的內容應包括個 資當事人個資被侵害之事實及本校已採取之因應措施，以及後續提供查詢及協助之方式。

(三) 如符合相關法令需申報之規範，個資委員會另應依法向主管機關提出申報。

(四) 事故發生後之個資正確性維護、錯誤之更正或整體環境之改善，由個資委員會責成相關單位進行討論及後續處理。相關單位於後續處理完成後，於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。

(五) 如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知當事人及取得其書面同意。