巧新科技工業股份有限公司

供應商資訊安全條款

1 供應商應設置負責並推動全公司資訊安全管理(含客戶機密資訊保護)之專責單位或主管。

2 供應商應制訂資訊安全政策與相關之管理規範，且其範圍包含客戶機密資訊保護、供應商、或下包商之資訊安全管理規範。

3 供應商員工在到職前公司均會進行學歷驗證、經歷驗證、或背景調查。

4 供應商員工在到職時均須簽署保密合約(NDA)，且其範圍包含客戶與本公司機密資訊。

5 供應商在職員工須定期接受資訊安全教育訓練並留下紀錄，而資訊安全教育訓練內容包含客戶與本公司機密資訊保護。

6 當供應商在職員工轉換單位或工作進行調整時，會根據工作需求立即予以移除/調整資訊存取權限、或繳回所持有之資訊資產。

7 供應商員工在離職前須將所持有的公司資產(含客戶與本公司機密資訊)繳回公司，此外公司亦會提醒其離職後的保密責任與義務。

8 供應商員工在離職後會立即予以移除其資訊存取權限、及門禁等所有實體安全權限。

9 供應商應執行釣魚郵件防範宣導與測試。

10 供應商存取公司內部資訊系統須通過使用者身分認證 (Authentication) 例如: 必須登入帳號密碼。

11 帳號與權限的申請與變更須有審核流程確保符合必須存取權限 (Need-to-Access) 原則。

12 供應商內部資訊系統須移除預設密碼 / 管控無須密碼的帳號。

13 帳號與權限須定期檢討與更新 (至少每年一次) 。

14 供應商依照帳號類型定義並要求密碼管理政策 ，包括: 密碼長度 >= 6 個字元、密碼複雜度（至少包含英文大小寫與數字）。

15 供應商依照帳號類型定義並要求密碼管理政策 :更改頻率週期 <= 6 個月。

16 供應商依照帳號類型定義並要求密碼管理政策 : 新更換的密碼不得與最近 3 次重複。

17 供應商依照帳號類型定義並要求密碼管理政策 : 密碼變更後最少三日後方可再進行變更。

18 供應商依照帳號類型定義並要求密碼管理政策 : 記錄帳號"失敗的嘗試登入次數"系統日誌，並設定帳號封鎖的條件 (例如:重複失敗 5 次) 。

19 供應商內之工作或存有重要資訊資產之場域均設有門禁管理(含防止尾隨)機制，且只允許事先被授權人員才能進入，其門禁管理具有個人身份驗證(如刷個人識別證或生物辨識)及防止尾隨機制，且所有門禁進出紀錄均會予以保存一段時間、管理單位並會定期檢視被授權人員名單與權限。

20 供應商內的出入口與重要區域均設置有 CCTV，且有專人負責維護與管理，CCTV 拍攝的影像均可清楚辨識人臉，且 CCTV 影像會儲存至少一個月以上。

21 禁止未經授權之攝錄影裝置(如私人照相手機)進入供應商之工作或存有重要資訊資產之場域，且供應商會執行檢查，並對違規者進行處置。

22 針對非供應商所擁有或授權之資訊儲存/複製/傳送裝置或媒體(如私人智慧型手機, 電腦, 硬碟, USB, 記憶卡, 燒錄機, 印表機, 傳真機等)訂有管制措施，且供應商會執行檢查，

並對違規者進行處置。

23 供應商應限制員工在外透過遠端連線至公司內部網路，須符合資安控管 : 只有必要人員執行必要功能並經過授權可遠端連線回公司 (例如: 緊急系統異常處理)。

24 供應商電腦老舊作業系統 (End of Support) 都有進行升級/汰換，可持續取得安全性更新(Security patch)，EOS 電腦若無升級/汰換請說明原因及風險管控方法或執行計畫。

25 供應商應建立公司電腦設備資產清單，並定期維護更新。

26 供應商電腦系統應安裝防毒軟體並持續更新版本與病毒碼。

27 供應商的對外網路(Perimeter & DMZ) 須有安全保護機制，包含 : 防火牆, Firewall。

28 供應商的對外網路(Perimeter & DMZ) 相關伺服器與應用程式須有安全防護措施 : 定期進行弱點掃描(Vulnerability scan)並修復漏洞。

29 建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常)之通報及處理程序，重大資安事件在 24 小時內通知受影響的客戶。

30 供應商宜取得外部第三方之任何資訊安全管理認證 (如 ISO 27001, ISO 15408, TISAX AL3…)

31 本公司保留對供應商執行資訊安全稽核之權利，得定期或於知悉供應商發生資訊安全事件時，對供應商執行資訊安全稽核，供應商應全力配合稽核，不得有任何異議。