台達資通安全執行情形

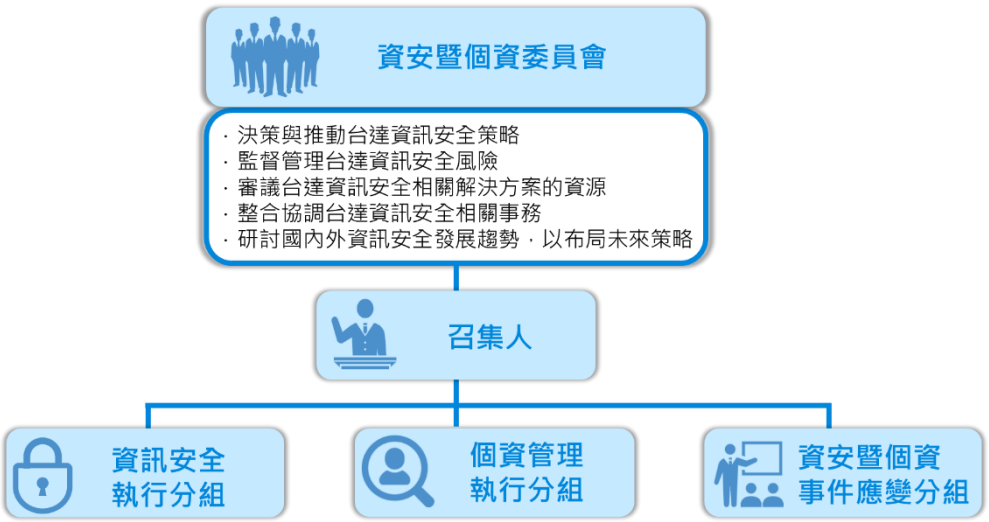
▶ 資通安全管理

(一) 資通安全風險管理架構

本公司已成立資訊安全委員會，由執行長擔任主席並由資訊長擔任資訊安全長，全球各事業群與各地區高階主管均為委員會委員；亦成立「資訊安全部」，專責台達集團資訊安全及實體安全規劃與相關的稽核事項，並促進此委員會運行。資訊安全委員會透過每季管理審查會議，審核資安風險分析結果及本公司採取對應的防護措施與方策，確保資訊安全管理體系持續運作的適用性、適切性及有效性。資訊安全長每年定期向董事會彙報資安管理成效及資安策略方向，以確保資訊安全政策與管控落實於台達集團全球各地區事業單位，於民國 113 年 4 月 30 日已向董事會報告資安治理執行情形。

(二) 資通安全政策

台達持續精進其資訊安全制度，並強化防護能力。透過成立「資訊安全暨個資委員會」來推動整體資訊安全治理，建立一致性的資訊安全政策，並規劃台達集團之資訊安全管理制度。台達由董事會負責核定集團資訊安全暨個資保護政策，以及決策資訊安全相關重大議題。所有資訊安全管理規範不僅需要符合國內外的資訊安全法律法規，還積極擴大國際資安標準的適用範圍和認證領域，將資訊安全融入日常業務的執行中。本政策每年會配合政府法令、環境、業務與技術之變動評估檢討，其修正須經董事會核定後公告實施。每年亦會針對集團員工，實施資訊安全政策及認知宣導，以加強同仁資訊安全意識。



(三) 具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

1. 組織控制
   - 台達訂立「台達集團資訊安全暨個人資料保護政策」，做為資訊安全暨個資管理組織權責分工、人員教育訓練、電腦硬軟體、網路及實體環境管理之準則。
   - 台達主要資訊系統於民國107年12月3日通過ISO/IEC 27001驗證，為持續確保資訊安全實施與維護證書有效性，每年實施包含資產盤點、風險評鑑與處置[1]、關鍵系統營運持續演練[2]、內部稽核[3]等控制措施。經外部驗證單位於民國113年7月12日以ISO/IEC 27001:2022 國際標準執行驗證通過，證書效期展延至民國116年8月8日，證書效期涵蓋民國113年度。我們將持續推動與落實資訊安全制度至台達集團全球各地區、各事業單位，以降低未知的資安風險，建立一個安全可信賴的資訊環境，從而保障集團和客戶的權益。

     註1：於113/1~113/3 完成風險評鑑作業。

     註2：於113/8 執行關鍵系統營運持續演練。

註3：於113/4~113/6 進行內部稽核。

- 為了確保資訊安全管理文件能夠與組織的實際運作相符合並因應資訊技術的不斷演變，台達在民國112年新增了5份管理辦法，並修改了9份程序文件。確保它們能夠有效地反映台達的最新需求和資訊安全標準。台達致力於持續提升其資訊安全管理水平，並確保其資訊系統和資料得到妥善保護。
- 透過國際資安大廠提供之專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為進階資安強化的依據。
- 為TWCERT成員，定期蒐集資安威脅情資，並做適當防範以降低公司可能暴露之風險。

2. 人員控制

在當今數位化和資訊化的環境中，資訊安全教育訓練被視為至關重要的一環。透過充分的資訊安全意識培訓，員工能夠更好地理解資訊安全的重要性，並學習如何預防和應對各種資安威脅。這包括學習如何避免常見的人為錯誤，並確保遵守相關的法規和標準。擁有這些資訊安全意識的同仁可以大大減少組織面臨的安全風險，提高數據和系統的保護水平，從而確保組織的業務運作安全可靠。

- 台達除對新進員工進行資安教育訓練，專業技術及管理單位人員亦須完成年度資訊安全教育訓練並通過測驗，民國112年度統計38,818人次完成年度資安線上與實體教育訓練，覆蓋率97%。資安部亦會不定期發行資安電子報，提醒員工最新的資訊安全風險、員工應注意事項等，資安部也設有資安專屬信箱，以利同仁發現資安問題時可即時反映。
- 為提升同仁資訊安全意識，每年定期對全球員工舉辦社交工程釣魚郵件演練、釣魚郵件辨識宣導，並分析演練結果以持續提升演練之有效性。民國112年度共執行48次釣魚郵件演練，共寄出 199,227 封郵件，全體員工平均的點閱率皆低於目標。

3. 技術控制

- 建置防毒系統，並搭配多層次資安監控機制，防止電腦病毒入侵風險。
- 導入SIEM (Security Information and Event Management) 系統並計畫部署端點偵測與回應 (Endpoint Detection and Response) 工具，以提升資安威脅偵測與回應的效率。
- 升級網路防火牆來達成網路防護與區隔，以強化關鍵基礎服務之安全管控措施。
- 佈署郵件安全閘道器Secure Email Gateway(SEG)，以阻擋駭客發送內含惡意程式或連結的釣魚郵件。
- 針對佈署於公司的應用系統，進行弱點掃描與管理，並因應數位化轉型與雲端安全性，推動更多的自動化整合方案以加強資安韌性。

(四) 投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

- 專責人力：設有專職之資訊安全主管 1 人及「資訊安全部」14 人，負責本公司資訊安全規劃、資安系統運作、技術導入與相關的稽核事項，以維護及持續強化資訊安全。
- 台達成立了「資訊安全委員會」，由執行長擔任主席，資訊安全長擔任召集人，營運長及全球各事業群與各地區高階主管均為委員會委員；每季定期召開會議，探討各地區面臨的資訊安全問題及業務需求並決定所需資源及執行方案。
- 台達於民國 112 年成立了「資訊安全推動委員會」，由各事業群指派主管擔任資訊安全推動種子，於定期的雙月會中，除了討論資訊安全相關議題外，亦透過此會議宣導總部正在推廣之資訊安全活動，藉此提升同仁資訊安全意識。

(五) 重大資安事件之影響及因應措施

對資訊安全事件的通報與處理，台達已明確訂立資安通報及處理流程，資安事件由資安維運管理小組進行收錄並訂定事件等級。相關單位需於目標處理時間內排除及解決資訊安全事件，並在事件處理完畢後進行根因分析與採取矯正措施，以預防事件重複發生。民國 112 年本公司未發生造成公司及顧客損失之資訊安全事件。