

大眾全球投資控股股份有限公司

資訊安全政策

2023 年 6 月 1 日訂定

第一條 (本政策之目的)

鑑於資訊安全乃維繫各項服務安全運作之基礎，為確保大眾全球投資控股股份有限公司（以下簡稱本公司）具備共識落實資訊安全的使命，並依「公開發行公司建立內部控制制度處理準則」第九條有關「電腦化資訊系統處理」之規範，及遵循 ISO 27001 資訊安全管理系統的管理框架，特訂定資訊安全政策（以下簡稱本文件），做為本公司資訊安全管理系統的最高指導原則。

第二條 (目標)

本公司資訊安全目標為確保核心系統管理業務之機密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability) 與法遵性 (Compliance)，並依各階層與職能定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

- 機密性: 應避免本公司任何敏感資訊洩露於網際網路。
- 完整性: 應確保本公司敏感資料 (如: 客戶資料、個人資料) 之正確性。
- 可用性: 應確保本公司所持有的重要資料確實備份。
- 法遵性: 應遵循我國相關法律 (如: 個人資料保護法、營業秘密法、智財權相關法律)，避免本公司或第三方人士權益受侵害。

第三條 (適用對象)

本「資訊安全政策」適用對象包含大眾集團各公司共用電腦機房和 ERP 系統之全體員工。

第四條 (管理資訊安全專責單位)

本公司管理資訊安全相關事宜之專責單位為資訊安全管理部，並主導「資安管理委員會」運行，推動及維持各類資安管理、執行與查核等工作之進行。其職權如下：

- 一、負責擬訂、修訂資安政策、目標及制度。
- 二、遵循 ISO 27001 框架進行資訊資產風險管理及資安制度執行和查核。
- 三、負責公司資訊安全政策推動、落實資安機制及提升公司員工資安意識。
- 四、負責擬訂與資安政策有關之所有文件、檔案及電子紀錄等資料之保

存。

- 五、營運持續計畫之規劃、評估與定期演練之實施。
- 六、建立與進行資安事故發生之事故通報機制。
- 七、資訊安全訊息內部之推廣、發佈與推廣相關之保護認知與宣導訓練。
- 八、蒐集、接收與更新外部之法令規範與標準訊息，並適時發佈提供內部同仁，可能影響企業營運、資訊安全等相關重要資訊。
- 九、跨部門資安議題溝通協調。
- 十、配合會計師事務所之查核團隊及外部專業驗證機構，進行資訊安全管理查核驗證，並依建議事項執行相關改善並持續追蹤。

第五條（實施原則）

資訊安全管理系統之實施應依據規劃（Plan）、執行（Do）、查核（Check）及持續改善（Action）循環模式，以週而復始、循序漸進的精神，確保資訊安全之有效性及持續性。

- 本政策應每年定期檢討，以反映政府法令、技術發展、業務需求及利害關係人影響等，以落實資訊安全作業的目標。
- 保護公司業務活動相關資訊，強化資料安全性，避免未經授權之存取與竄改等不當使用之情事。
- 資訊資產（包括軟體、硬體、網路通訊、資料及人員等）應予適當保護，並每年定期評鑑風險予以改善。
- 訂定備援回復等措施，定期演練，確保本公司重要資訊管理系統可維持穩定可供服務使用。
- 建置資訊安全監控自動化與強化防禦預警能力，降低資訊遭受未經授權之入侵、惡意破壞或洩露等攻擊行為。
- 確實落實日常運維之標準化作業程序，並定期進行內部稽核及外部查核，確保內部控制制度及相關作業程序之有效性。
- 所有發生資通安全事件或遇到可疑之安全事件，應即時依「資安事件事故管理作業規範」進行通報，以使專責單位數予以調查及處理。
- 第三方委外廠商及訪客，應遵守「第三方管理作業規範」，如有接觸本公司相關資訊應簽署「第三方保密切結書」以保護本公司資訊資產之安全性。
- 提供資訊安全教育訓練，強化員工之資訊安全意識及其對相關責任之認知。

第六條（審查與評估）

- 一、本文件應至少每年評估審查一次，考量法令法規、科技變化、關注方期望、業務活動、內部管理與資源等最新現況，確保資訊安全實務作業之有效性。
- 二、本文件應依據審查結果進行修訂，並經資安委員會主委發佈後始生效。
- 三、本文件訂定或修訂後應以適當方式（例：E-Mail 或網站公告或紙本印

出)告知利害關係人,如:所屬員工、供應商、客戶、外部稽核人員等。

四、資訊安全之相關檔案文件,應備份並保存於安全之處所。

第七條 (資訊安全手冊)

依據本公司「資訊安全政策」及相關規範,另制定「資訊安全手冊」,做為資訊安全管理系統(Information Security Management System)的準則,內容請參閱已發行的 ISMS-01-02_資訊安全手冊。