113 年 9 月 10 日

資通安全政策

本公司為充分運用資訊及通訊安全科技，建構兼具有效性及完整性之資通安全防護機制，以確保資訊資產之機密性、完整性及可用性。

範圍與聲明

本政策適用於本公司業務、受託業務及其他與個人資料相關之各項服務。為達本公司對資通安全維護的期許與要求，本公司將以資通安全政策為基 礎，依據組織發展需要，並考量資訊資產風險，建立一個完整、可行、有效 的資訊安全管理系統，以為本公司資通安全提供最佳之保障。

資通安全推動組織

1、 為統籌資通安全工作之執行，以整體性資通安全角度，規劃與管理資安風險，本公司於數位暨資安部下設資安治理組與資安防禦組，專職辦理資通安全業務，各部室落實執行各項資安作業，提升本公司資安維護能量。

2、 本公司由督導資通安全專職單位之副總經理擔任資訊安全長，審核資安業務會報議程及核閱會議紀錄之內容，及督導資通安全相關事項。

資通安全防護機制

1、 本公司各資訊系統之軟硬體、網路及資安相關設備由資訊部門負責維運作業，並依據法令法規、主管機關及內外部利害關係人要求，以及考量外在科技環境威脅與本公司業務運作所需，建置各項資訊防護、控制措施與監控管理機制，對本公司各資訊系統與設備，採取必要且適當之防護與監控，以確保各系統與設備運作正常。

2、 本公司全組織導入資訊安全管理系統(Information Security Management Systems, ISMS)，管制措施需符合 ISO/IEC 27001:2022 及 CNS 27001:2023 之規範，並通過第三方驗證。

3、 本公司全組織導入臺灣個人資料保護與管理制度規範(Taiwan Personal Information Protection and Administration System,TPIPAS)，並取得資

料隱私保護標章。

業務持續運作

為確保本公司主要作業於遭遇重大災害時，得於預期的時間內復原，建立業務永續運作計畫，明確鑑別本公司關鍵作業、重要作業及一般作業所需的人力及資源，以確保有足夠的人力及資源來進行災害的預防準備及緊急應變，提供復原行動的執行步驟，以確保必要的恢復工作得及時依序執行，並透過測試演練確認業務永續運作計畫之符合程度與妥適性。

資通安全事件應變

1、 對各項訊息與警訊進行監控，分析其是否需進行追蹤，以判定有無潛在風險，期儘早研擬因應措施，降低資通安全事件發生之可能。

2、 若發生資通安全事件時，本公司遵循「資通安全事件通報及應變辦法」辦理，即時掌握資通安全事件，立即通報與採取適當應變措施，評估與控管事件影響之範圍，以降低事故損害。

網路安全提醒

1、 避免連線安全性低之公用網路。

2、 避免安裝來源不明的 APP 或移除來源不明的 APP。

3、 避免於不安全的電腦設備或手機進行個人帳號登入等相關操作。

4、 電腦或手機安裝防毒軟體或防火牆以防止駭客入侵，並經常更新防毒軟體與病毒碼。

5、 請勿點選不明網站及下載不明程式，如網頁、電子郵件畫面上顯示的連結網址勿隨意點選；電子郵件、即時通訊傳送的附件檔案勿隨意開啟。

6、 本公司 APP(集保 e 手掌握)請從 App Store® 或 Google Play™之平台下載安裝。