桂盟國際股份有限公司

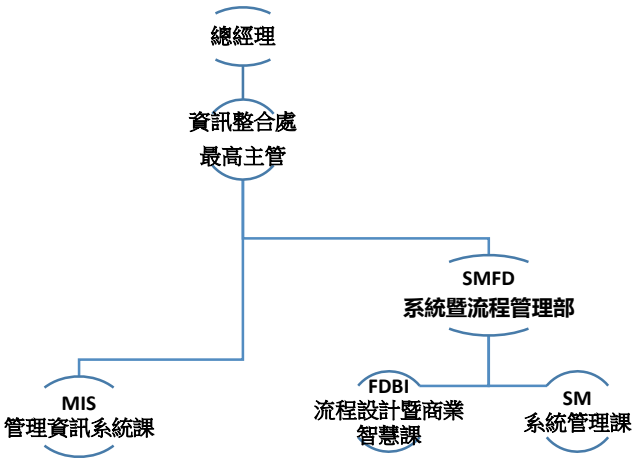
資訊安全政策

一、資訊安全目的與範圍

桂盟國際股份有限公司（以下簡稱本公司）為維護公司整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性，並建立安全及可信賴之作業環境，確保資料安全、系統安全、設備安全、網路安全，保障本公司同仁與相關內、外部人員之權益，特訂定本政策。

二、資訊安全風險架構

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立【資訊整合處】， 由總經理及資訊整合處最高主管負責監管執行。該組織團隊負責執行資訊安全系統建置，包含網路管理與系統管理並配合公司稽核單位進行資訊安全稽核工作，包含內部稽核與外部稽核。



三、資訊安全政策目標

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。

A. 資訊安全之範圍：

（1）人員管理及資訊安全教育訓練。
（2）電腦系統安全管理。
（3）網路安全管理。
（4）系統存取管制。
（5）系統發展及維護安全管理。
（6）資訊資產安全管理。
（7）實體及環境安全管理。

(8) 資訊系統永續運作計畫管理。

(9) 資訊安全稽核。

B. 資訊安全的原則及標準：

(1) 定期進行資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、 資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊 安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。

(2) 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

(3) 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

C. 員工應遵守之相關規定：

(1) 資訊單位接收帳號申請單後，建立「使用者代號」。

(2) 電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，以維護資料完整性。

(3) 禁止使用非法版權軟體。

(4) 進入主機後，若作業結束或長時間不使用設備時，應鎖定或關閉主機，以免資料機密外洩，為別人所破壞或造成當機之困擾。

(5) 電腦設備之擺放位置除以方便為原則外 ，應遠離茶水、咖啡、日曬或潮溼地點，以延長其壽命。

(6) 離職或新舊職務交接時，由資訊單位衡量資料相關性作適當處置。

(7) 電腦設備無法正常作業時，使用者應立即通知資訊單位，以便檢查或維修。

四、資訊安全控制措施

項目	具體管理措施
防火牆防禦	● 防火牆設定連線規則。 ● 如有特殊連線需求需額外申請開放
使用者上網控管機制	● 使用自動網站防護系統控管使用者上網行為。 ● 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	● 使用企業級防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	● 作業系統自動更新，因故未更新者，由資訊部協助更新。
郵件安全管控	● 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔

	案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 ● 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
資料備份機制	● 重要資訊系統資料庫皆設定每日備份。 ● 進行多處異地備援機制。
機密性資料權限控管	● 公司內各部門重要檔案存放於內部網路儲存設備，並依循部門員工權限進行資料夾權限控管，避免共用資料導致機密資料外洩。
系統復原計劃制度	● 重大事故系統復原，可由資訊管理部門與電腦廠商簽訂重大意外事故之系統復原合約，合約內容應包含到達時效、維修時效、若無法在可接受的時間內完修須以備品替代等條文。 ● 判定系統故障之因素，屬於硬體問題或軟體問題。若屬硬體問題，應洽廠商進行檢測維修，並對復原後系統進行測試、驗收；若屬軟體問題，則應與相關單位討論發生原因，並追查是否有人為疏失，必要時洽廠商或資訊管理部門重新安裝。 ● 對備援設備應不定期測試其可用性
資安險	● 本公司於評估市面資安險種保險範圍、適用行業等項目後，暫不投保資安險，但因應資訊安全所面臨的挑戰，已導入相關軟硬體,例如防火牆、防毒、入侵防護系統…等，並持續關注資訊環境變化趨勢，並強化公司同仁資安危機意識及資安處理人員應變能力。

五、緊急通報程序

當發生資訊安全事件時，發生單位通報資訊安全處理小組，判斷事件類型並找出問題點，即時處理並留下紀錄。

六、114 年度辦理資訊安全宣導執行情況

- 資安宣導:

  本年度進行兩次資訊安全宣導事項:

  114/4/17 【KMC-資訊整合處】114 年社交工程釣魚郵件演練事件宣導

  114/11/20 【KMC-資訊安全宣導】釣魚郵件及詐騙防範宣導