為落實經營者的責任，促進經營績效、保障投資者權益。宏盛善盡資訊安全治理之責任，掌控資訊安全與企業風險管理，保護公司之成果資料、策略、合約文件、智慧財產、資訊系統等企業重要資產，或是資訊安全策略與內部控制，持續對資訊安全精進治理與強化防護能力，以確保公司永續營運之基礎。

資訊安全政策

資安政策主軸聚焦於紮根資安基礎、落實制度規範及資訊技術應用三個層面來進行，從內部資通安全管理辦法、並透過資訊科技主動通報資安風險事件，人員到組織全面提升資安意識。

1. 紮根資安基礎：
   定期檢視及升級網路基礎架構環境、持續修補內部系統潛在弱點、定期演練災難還原機制，實施人員資安全教育訓練實務課程，全面性的深化資安基礎防禦力。

2. 落實制度規範：
   訂定公司資訊安全管理制度，定期審視及檢核資安內控執行成效，並貼合國際資訊安全規範，落實資訊安全控管機制之運行。

3. 資訊技術應用：
   持續導入資訊安全設備及資安技術應用，透過如即時告警系統、端點防護系統、弱點掃描、入侵偵測聯防等技術應用，預先掌握資訊風險狀態，提升資安防禦立即應變能力。

管理架構

- 本公司管理部資訊科為資訊安全之主責單位，負責訂定、推動與落實資安政策與資訊安全作業，由管理部主管行必要之統籌、規劃暨執行相關事宜，並定期(至少一年乙次)向董事會報告資安治理概況。

- 本公司稽核室為資訊安全風險之督導單位，依據內部控制制度之電子資料作業處理循環每年定期執行資訊安全檢查。若有發現缺失或是資安事件，立即通知部門主管，要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低資安風險。

資訊安全具體管理機制

項目	具體措施
電腦設備安全管理	(1) 電腦主機、伺服器等設備均設置於專用機房，機房門禁採用感應刷卡進出，僅限公司資訊人員及其單位主管進出，其餘人員則需填寫機房出入登記簿存查。 (2) 機房配置不斷電與穩壓設備，市電中斷時自動啟動關機程序，避免意外瞬間斷電造成系統當機。
網路安全管理	(1) 配置防火牆，並定期檢討電腦網路安全控管事項之執行。 (2) 使用防毒軟體，並自動更新病毒威脅碼，降低病毒感染機會。 (3) 電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的 PC。
系統存取控制	(1) 網路儲存區及各應用系統依個人、部門、公共及系統等層級分別設定使用權限，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊室建立系統帳號後方得存取。 (2) 帳號的密碼設置，規定適當的強度、字數，並且必須文數字、特殊符號混雜，才能通過。 (3) 同仁辦理離職、退休或調動程續時，由資訊室進行各系統帳號的刪除或權限調整作業。

項目	具體措施
確保系統的永續運作	(1) 系統備份：建置雲端備份系統，採取日備份機制，除了上傳一份於代管機房儲存外，電腦機房及儲存媒體均另各存一份複本，以確保系統與資料的安全。 (2) 災害復原演練：各系統每季實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，再由系統測試確認回復資料的正確性，確保備份媒體的正確性與有效性。 (3) 租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。
資安宣導與教育訓練	(1) 提醒宣導：資訊室同仁每月均精選與業務相關之資安宣導文章並以內部系統公告，以提升全體同仁對資訊安全危機意識與應變能力。 (2) 教育訓練：不定期透過外部教育訓練提升資訊人員的專業職能。

註: 本公司尚未投保資安險，未來將配合法令規定予以執行