資訊安全風險管理架構，訂定資訊安全政策及具體管理方案

功能職責劃分

- 本公司資訊單位為專責系統安全管理，Nas 系統維護管理及備份、監視器系統維護管理、Eset 防毒系統維護管理、網域及網路裝置維護管理、郵件伺服器維護管理、Terminal Server 系統維護管理、防火牆維護管理、印表機及電腦周邊維護管理、偉盟系統(SQL)、共用區及 Mail 收件夾備份、系統權限控管、協助各會議之視訊設備操作及相關錄音檔、影音檔轉檔、燒錄。資訊部僅執行資訊權責工作。資訊人員離職後，資訊人員離職當日將系統中離職之資訊人員之帳號刪除。公司內部人員職務或工作異動時，資訊人員於員工離職當日將系統中離職員工之帳號刪除。員工離職時，員工離職將其工作進度及保管物品填寫「工作交接清單」含電腦資料檔案及「物品交接清單」一併辦理交接。

資訊安全政策及具體管理方案

- 確保本公司軟體、設備及網際網路之安全，均定期宣導資訊安全管理政策，各部門需使用經授權之合法軟體，並遵守相關法令及契約規定，非經合法授權及與業務無關之軟體，不得安裝使用，違者除應擔負有關法律責任外，倘若導致各單位設備毀損，尚應負相關損害賠償責任，作為本公司全體員工遵循資訊安全之依據。同時為確保各項資訊系統免受任何內、外部因素之干擾、破壞、入侵或任何不當使用或蓄意破壞之行為，須經由適當的系統規劃、程序規範及行政管理，以防範來自內、外部的威脅，達到維護資訊系統安全的目的。公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。由資訊單位負責統籌資訊安全及相關事宜，並由稽核室擬定相關內部控制程序管理及定期進行內部稽核。
- 已正式作業之系統均具備應有之系統文件、程式文件及使用操作手冊。電腦文書應包括:(1)系統關聯圖(2)無自行開發或修改之程式文件(3)操作手冊統籌由資訊部門負責保管。偉盟系統各作業系統均建置操作手冊供使用單位參考。
- 程式之存取(1)需求提出須由需求單位主管核可。(2)須確實做過可行性評估。(3)須做過成本效益評估。(4)須完善執行專案時程控制。(5)須依據系統分析的結果以確認與使用者之需求相符。(6)須確認程式設計完全符合系統需求單所述。
- 資料之存取(1)對資料檔案的存取使用，均有詳細的書面管制說明。(2)嚴格禁止由非負責程式開發/維護人員負責使用者權限資料之更新作業。(3)嚴格控管使用權限，均設置使用識別碼及密碼，限制各終端機使用者，僅能利用其本身經核准單獨使用之識別碼及密碼，開啟或接觸其經核准使用之資料檔案。(4)凡各單位使用人員之新增、工作異動或離職任用及調職均需填寫「應用系統權限申請單」，以確保資料存取

之授權範圍。(5)凡各單位使用人員離職，人事單位確實會辦資訊單位，確保資料及時更新。資訊單位專職人員依權責主管核決後之「網路帳號申請單」維護使用者之權限。每一使用者於終端機均設有專屬帳號與密碼，且帳號密碼不得與他人共用。員工離職之「移交手續清單」、「應用系統權限申請單」均會辦資訊單位並確實執行系統使用權限之維護。

- 資料輸出：(1)均有合宜之權限控管。(2)輸出資料均妥善保存。(3)逾期或作廢無效之輸出資料均進行銷毀。(4)均建立系統產生單據或報表之分發程序。資訊單位專職人員依權責主管核決後之「應用系統權限申請單」維護使用者之權限。資料輸入：(1)輸入資料(原始單據)之編製、核對及覆核均予適當分工。(2)應對不同使用單位及人員之權限，訂定不同等級提供其授權使用之輸出報告、報表。(3)輸出較具有高度敏感性及機密性之報表時，均指定專人負責分送及指定專屬印表機，以確保機密資料之安全。(4)確認輸入資料正確無誤。(5)應用程式的輸入均有欄位合理性檢查。(6)資料輸入完成後均再次檢查其正確性。資訊單位專職人員依權責主管核決後之「應用系統權限申請單」維護使用者之權限。系統使用者權限均依職責分工而作區別。印表機設定為公共使用與專用。輸入資料經系統合理性檢查並依職責權限審核後完成。
- 錯誤更正：規範已登錄系統後，資料之修改或輸入錯誤之更正及核准程序。系統使用者權限均依職責分工而作區別。惟基於風險控管原則，刪除權限由單位主管執行。
- 資料處理之控制(1)應用程式均提供操作手冊。(2)應用程式均設有防錯處理。(3)均規範系統應提供使用者作業處理中各項錯誤或作業失敗之訊息。應用程式操作手冊電子檔存放於公用資料夾-管理部-各部門共用表單-採購部-資訊表單中，供各單位下載參閱。操作人員操作錯誤時，會跳出錯誤的訊號，並且無法完成資料輸入。
- 檔案及設備之安全設備控制(1)各部門系統作業資料皆存放於File Server。(2)檔案資料每日均確實做備份，由資訊人員保管。(3)申請檔案權限者均應由部門主管審核後交資訊部開放權限。(4)對外線路主機是均做好防護措施，公司網路設有防火牆措施，防止外部入侵。(5)資訊人員負責備份資料至其他主機，一份備份在隨身硬碟。(6)電腦機房非資訊人員未經核准不得進出機房。電腦機房門禁設置指紋機僅供資訊人員使用。外部人員(如保全)進出機房需填寫「機房進出管制紀錄表」並由資訊人員陪同進出。(7)電腦主機集中於機房，由資訊部門負責保管。(8)電腦機房設有冷氣設備防止溫度過高，影響設備運作，且裝有UPS設備。
- 系統復原計劃制度及測試程序之控制(1)隨時可以恢復主機功能。(2)由資訊人員負責備份一份至其他主機。(3)資訊部備有「緊急應變暨系統復原計劃」。
- 資通安全檢查程序之控制(1)與外界間之資料交換是否有適當的安全控管。(2)對外連結的主機或設備均有適當的防火牆做安全管制，作網路安全控管。(3)新進人員填寫

「網路帳號申請單」應經權責主管核准簽章後交付資訊單位開放並告知郵件使用之規定。員工離職時，均依離職手續，會辦資訊單位，資訊單位將離職人員帳號刪除。

- 資訊單位定期就現有及未來規劃之資訊軟硬體的需求及系統使用規模與資料儲存量需求，評估資安風險造成損失之可能性，必要時投保適當之保險以降低損失金額。