資訊安全風險管理架構

本公司為全面導入資通安全體系，於 112 年成立資通安全政策推行小組，並配置資安專責主管 1 名及 1 名資安專責人員，主係確保資通安全管理制度之運作，鑑別資通安全管理制度之內、外部議題及利害相關團體對本公司之資通安全要求與期望。

資通安全風險管理架構

1. 由本公司資訊主管成立資通安全管理小組，資訊部門負責主導及規劃，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
2. 本小組負責制定資通安全管理政策，定期檢討修正。
3. 本小組定期召開會議檢討執行情形，並每年定期向董事會報告執行情形與檢討。

資通安全對象與範圍

對象：包括員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。
範圍：為確保本公司資通安全，制定相關規章制度，應用技術和數據安全標準制定， 並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與 資通安全維護。

資訊安全政策

一、公司為管理資訊安全之風險，已訂定資訊安全政策與資訊安全管理措施。

二、電腦設備安全管理

1. 本公司各應用伺服器等設備均設置於專用機房，機房進出保留進出紀錄存查。
2. 機房主機配置不斷電與穩壓設備， 避免台電意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

三、網路安全管理

1. 與外界網路連線的入口，配置防火牆，阻擋駭客非法入侵。
2. 同仁由遠端登入公司內網存取系統，必須申請VPN帳號，透過VPN的安

全方式始能登入使用。

四、病毒防護與管理

1. 伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。
2. 建置垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的電腦。

五、系統存取控制

1. 同仁對各應用系統的使用，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，由資訊部建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。
2. 帳號的密碼設置，規定適當的強度。
3. 同仁辦理離職手續時，由資訊部進行各系統帳號的刪除作業。

六、確保系統的永續運作

1. 系統備份：建置備份管理系統，採取日備份機制，並建置異地備援。
2. 災害復原演練：每年實施二次災害復原演練。

七、資安宣導與教育訓練

1. 定期宣導。每季要求同仁定期更換系統密碼，以維帳號安全。
2. 定期實施資訊安全教育訓練宣導，資訊安全政策及相關實施規定。

資訊安全具體管理方案

一、 防火牆防護

1. 防火牆設定連線規則。
2. 如有特殊連線需求需額外申請開放。

二、 使用者上網控管機制

1. 使用自動網站防護系統控管使用者上網行為。
2. 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。

三、 防毒軟體

使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。

四、 郵件安全管控

1.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。

2. 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。

五、 資料備份機制

1.重要資訊系統資料庫皆設定每日備份。

2.建置異地備援。

資通安全的資源投入

資通安全由本公司資訊處負責，共設置 2 人，針對資通安全管理每季會議檢討。針對系統主機的作業系統或重要軟體升級、災害復原演練等重要的資安工作，資訊處每季檢討規劃執行， 並透過不定期的資安健檢，判斷資訊設備資源投入與系統配置是否存在漏洞，編列資安預算後執行。

緊急通報程序

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