資通安全管理

資通安全風險管理架構：

本公司資訊安全之權責單位為資訊部，設置資訊主管一名及專業資訊工程師兩名，負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關之資訊安全作業。

本公司稽核室為資訊安全監理單位，若查核發現缺失，即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低資訊安全風險。

資通安全政策與管理方案：

為強化資通安全管理，確保資訊的機密性、可用性以及完整性，並免於內部、外部的蓄意或意外的威脅，資通安全政策管理方式分為六大面向，闡述如下：

1.電腦設備安全管理

(1)本公司電腦主機、各應用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，且保留進出紀錄存查。

(2)機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並配置自動滅火系統，可即時降低機房火災所引起之災害。

(3)機房主機配置不斷電與穩壓設備，並連結公司大樓自備的發電機供電系統，避免市電意外瞬間斷電造成系統當機，確保電腦應用系統的運作。

2.網路安全管理

(1)強化網路控管，與外界網路連線的入口，配置企業級防火牆，阻擋駭客非法入侵。

(2)台北總公司與外部各據點採用專線連線作業，使用資料加密的方式，避免資料傳輸過程遭受非法擷取。

(3)同仁由遠端登入公司內網存取電腦應用系統，必須申請 VPN 帳號，透過 VPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。

(4)配置網路管理設備，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。

3.病毒防護與管理

(1)伺服器與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)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終端電腦設備。

(3)防病毒系統對於所偵測或攔截到的病毒，除立即予以隔離或刪除外，並主動發出受感染和處於風險的電腦風險報告，以利管理人員採取因應行動。

4.系統存取控制

(1)終端電腦設備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，規定適當的強度才能通過，並且設置密碼輸入錯誤帳號鎖定機制。

(3)同仁辦理離(休)職手續時，必須會辦資訊部，進行各系統帳號的刪除作業。

5.確保系統的永續運作

(1)系統備份：建置備份系統，採取日備份機制，系統與資料庫一份於電腦機房及異地均另各存一份，以確保絕對的安全。

(2)災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，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)租用電信公司數據線路，透過頻寬管理設備，數據線路並聯互為備援使用，確保網路通訊不中斷。

6.資訊安全宣導

(1)宣導要求同仁避免使用不明的網路網站，以維護資訊安全。

(2)不定期對內部同仁宣導資訊安全相關訊息及最新資訊安全情報。

投入資通安全管理之資源：

為實踐六大項資通安全政策，投入之資源如下：

1.網路硬體設備如防火牆、郵件防毒、垃圾郵件過濾。

2.軟體系統如端點防護系統、備份管理軟體、VPN 認證及加密軟體等。

3.電信服務如多重線路、異地備份、入侵防護服務等。

4.投入人力如：每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行、每年系統災難復原執行演練、每年對資訊循環之內部稽核等。

5.資安人力：資訊安全主管一名及資訊安全人員兩名，負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂。