資訊安全風險管理與運作情形

本公司資訊安全之權責單位為資訊部，設置資訊主管一名，及專業資訊工程師數名，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。

基於資訊安全的重要性，權責單位每年定期向董事會報告公司資訊安全治理與執行狀況。

一、 資訊安全政策目標：

1. 維持各資訊系統持續運作。
2. 防止駭客及各種病毒入侵及破壞。
3. 防止人為意圖不當及不法使用。
4. 防止機敏資料外洩。
5. 避免人為疏失意外。
6. 維護實體環境安全。

二、 資訊安全控制措施

1. 電腦設備安全管理

(1)本公司電腦主機及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)機房內部空調具有備援機制，可維持電腦設備於適當的溫、濕度環境下運轉；並放置 FE-13 環保氣體全自動電腦滅火系統，可適用於一般或電器所引起的火災。

(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。

2. 網路安全管理

(1)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)台北集團總部與海外廠:昆山、深圳及越南廠的連線作業，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 ERP 系統，必須申請 SSLVPN 帳號，透過 SSLVPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。

(4)配置上網行為管理與過濾設備，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)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。

4.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、字數，並且必須英文、數字、特殊符號混雜，才能通過。

(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：建置雲端備份系統，採取日備份機制，除了上傳一份於 Hicloud Boxe 雲端儲存服務外，電腦機房存一份複本，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，再由使用單位書面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。

6.資安宣導與教育訓練

(1)提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。

(2)講座宣導：每年對內部同仁實施資訊安全相關的教育訓練課程。

三、 110 年度執行情形

- 每天執行異地備份。
- 本年度辦理 1 次災害還原演練
- 教育教練：
  共舉辦 11 場「防毒軟體教育訓練」、「垃圾郵件過濾軟體操作教育訓練」、「勒索病毒說明與防範」、「資安教育訓練」等資訊安全教育訓練課程，累計宣導時數 80 小時，累計參與人數 46 人次。