114 年資訊安全風險管理措施及執行情形

一、資訊安全風險管理架構

公司資訊安全由資訊部負責統籌資訊安全及相關事宜，訂定資安規範與資安的推動與落實。每年定期由稽核室每年依照內控制度 「電腦化資訊系統管理作業」進行內部查核作業確保公司資訊作業內部控制之有效性及向董事會報告。

二、資通安全政策

為落實資安管理，本公司訂有「資訊作業安全實施要點」以作為資通安全風險管理之依據，藉全體同仁共同努力期望達成下列政策目標。

- 透過資訊安全管理，保障公司及客戶的各項權益。
- 確保資訊使用範圍內，所有項目之完整性、可用性及機密性。
- 定期進行資安宣導及教育訓練，加強員工資安常識。
- 定期檢視關鍵性資訊設備及災難復原計劃演練，以確保公司業務持續運作。
- 依據各職能資料存取需經審核，防止未經授權的資料被修改。
- 貫徹上述目標，業務永續經營。

三、具體資訊安全管理措施

本公司考量資安險仍屬新興險種，目前尚無適合本公司之資安險，故現階段以本公司既有的資訊安全管理程序來落實資訊安全風險管理。相關具體執行措施如下：

類型	管理作業
網路安全管理	• 配置企業級防火牆，阻擋駭客非法入侵。 • 與分公司各點使用 MVPN 的連線作業，使用資料加密方式，避免資料傳輸過程遭到非法擷取。 • 配置上網行為管理系統，控管網路存取，可屏蔽訪問有害或政策不允許的網址及內容，強化網路安全且防止頻寬被不當佔用。
系統存取控制	• 公司內各應用系統的使用，需透過資訊服務需求申請程序，經權責主管核准後，由資訊室建立帳號，且經過各系統管理員依所申請之功能開放權限，方得使用。

	・帳號的密碼設置，需符合規定之強度，且需文數字參雜，才能通過。 ・同仁辦理離職手續時，需會辦資訊部，進行各系統帳號刪除作業。
落實資安訓練	・新進人員教育訓練中加入資安宣導。 ・定期加強資安宣導，強化同仁資安概念。
病毒防護與管理	・伺服器與同仁電腦設備皆安裝端點防護軟體，病毒碼採自動更新，確保能阻擋最新型病毒。 ・電子郵件伺服器配置有垃圾信過濾機制，防堵病毒或垃圾郵件進入使用者端 PC。
確保系統可用性	・建置備份管理系統，定期將每日備份的資料，一份保留在機房，另一份放於異地，互相備援。 ・定期實施災難復原演練，選定還原基準點後，由備份檔回存於系統主機。
電腦設備安全管理	・本公司電腦主機、各應用伺服器……等皆設置於專用機房，機房門禁採感應式刷卡進出，且保留記錄存查。 ・資訊機房內有獨立空調及不斷電系統，其中不斷電系統與發電機串聯，停電時可由發電機供給不斷電系統電源，以維持電腦設備於適合的溫度下運轉，斷電時不會中斷電腦應用系統的運作。
檢核	・稽核單位每年定期查核，確保管制程序之有效性。

四、資通事件處理與通報：

公司已建置資安事件處理標準程序，明訂相關流程與措施。

五、投入資通安全管理之資源:

(1)每日防毒報告監控與問題電腦處理。

(2)每日網路監測與防火牆資訊監測。

(3)每年配合稽核單位執行系統人員權限審閱。

(4)異地備緩機制建立。

(5)郵件系統防垃圾郵件系統建立。

六、資通安全執行狀況：

(1)114 年度本公司執行資訊設備維護更新投入經費約 169,768 元。

(2)所有新進員工皆於到職後完成資訊安全教育訓練課程；資安人員接受外部教育訓練免費課程 6 小時。

(3)公司系統除執行版本更新和台電停電期間短暫無法使用外，114 年度無因重大資通安全事件所遭受之損失。無重大資安事件導致營業損害之情事並持續落實執行。