潤隆建設股份有限公司

資訊安全風險管理

經本公司權責單位評估，資訊安全風險雖非屬於本公司重大營運風險項目，但考量網路環境漸趨複雜，相關風險可能逐年增高，本公司管理資訊人員隸屬管理部並為資訊安全管理之執行單位，進行資訊安全預防及危機處理等具體管理方案，並實施對應的安控措施，持續精進內部異常偵測與防護方法，以降低企業資安風險。本公司每年至少一次向董事會報告「資訊安全風險管理情形」。

一、資訊安全具體管理方案：

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：

1.網路安全管理：

(1)配置企業級防火牆，阻擋駭客非法入侵。

(2)與北中南分公司使用 Hi-Link VPN 企業專屬線路作業,使用資料加密方式，避免資料傳輸過程遭到非法擷取。

(3)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。

2.系統存取控制：

(1)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。

(2)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。

(3)同仁辦理離職手續時，需會辦管理部資訊人員，進行各系統帳號及權限的刪除作業。

3.落實資安訓練：

(1)新進人員教育訓練中加入資安課程。

(2)在職同仁教育訓練，每季針對違反資安規定之同仁再特別開課訓練。

4.病毒防護與管理：

(1)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。

(2)電子郵件伺服器配置有廣告垃圾信過濾機制，防堵病毒或垃圾郵件進入使用者端 PC。

5.確保系統可用性：

(1)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（台中分公司機房），互相備援。

(2)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。

6.電腦設備安全管理：

(1)本公司電腦主機、各應用伺服器.....等皆設置於專用機房，機房隨時上鎖嚴格控管人員進出，且保留記錄存查。

(2)資訊機房內有獨立空調及不斷電系統，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。

(3)建置設備管理系統，需經過公司認證之移動裝置及 USB 裝置才可連線至公司內網及存取資料。

二、資訊系統損害對公司業務之影響與因應措施：

目前公司資訊系統架構中，在硬體部份是建置高穩定性伺服器，而軟體部份則是定期將資訊系統、軟體與系統設定參數做映像檔案備援及完整資料備份機制以確保縮短服務中斷時間。

在資訊服務不中斷及資料安全上，管理部資訊單位定期將備份資料送往異地保管存放，並定期演練災後復原措施，以預防及降低無預警天災以及人為疏失帶來的資訊服務中斷和縮短系統復原的時間。

為了資訊系統在發生損害時能順利恢復業務運作減少損失，除了定期演練災後復原措施之外，應隨著新興科技技術不斷發展來規劃設計與提升軟硬體設備資源，建構安全等級更高的防護機制以降低系統損害風險。

近來資安威脅分析，其威脅來源來自外部駭客攻擊佔大宗，其次是內部員工的疏忽及欠缺資安意識，而這些造成資安事件的根源，就是使用者開啟並點選釣魚電子郵件與執行不明惡意程式所造成，因此資安防護需要公司的全面共識和全員參與，惟有從工作習慣與公司文化，逐步養成員工的風險意識與資安防護能力，才能真正強化資安防禦能力。

三、110 年度本公司並未發現任何重大的網絡攻擊或事件，已經或可能將對公司業務及營運產生重大不利影響，也未曾涉入任何與此有關的法律案件或監管調查。