潤隆建設股份有限公司

114 年資訊安全風險管理及執行情形

一、資通安全風險管理架構

目前本公司資訊人員隸屬管理部並為資通安全管理之執行單位，進行資通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。

本公司因應「公開發行公司建立內部控制制度處理準則」規定，於 112 年 12 月底前完成配置資訊安全主管及至少 1 名資訊安全人員，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。

每年至少一次向董事會報告「資訊安全風險管理情形」。

二、資通安全政策

1.法規遵循：本公司執行業務時應遵守政府資通安全與個人資料保護相關法規及標準。

2.安全教育：定期實施資通安全教育訓練，宣導資通安全政策及實施規定。

3.規劃資源：建立資訊資產管理機制，統籌分配並有效應用資源，解決安全問題。

4.事先防範：新資訊系統或服務建置或推出前，應納入資通安全因素，以防範危害安全情況之發生。

5.安全監控：建立資通安全監控與防護措施，並定期進行檢視。

6.授權管理：明確規範資訊系統、網路服務、敏感資訊之使用權限，防止未經授權存取之行為。

7.檢討改善：訂定及執行內外部稽核活動，以落實資通安全管理制度，並針對未盡事項執行改善。

8.業務持續：訂定資通安全之營運持續計畫並實際演練，確保突發事故發生時得以應變。

9.資安文化：所有人員皆負有資通安全之責任，且應瞭解及遵守相關之資通安全規定，並於工作職責中落實。

目前本公司非依規定需要就資安政策及具體管理方案取得國際認證要求之公司，依本公司資訊單位辨識的資訊安全風險胃納程度，尚不需針對資安風險進行投保。

三、資訊安全具體管理方案：

本公司目前尚未投保資安險，故現階段以本公司既有的資訊安全管理程序來落實資通安全風險管理。相關具體執行措施如下：

1.資通安全管理：

(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 HiLink 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)配置電子資料控管系統，控管對內外網路通訊，監控網路流量狀況可強化網路安全並屏蔽訪問有害或政策不允許的網址及內容,更能防止頻寬不當佔用，達到傳輸控管防止資料外洩及病毒外洩。

(4)公司為台灣電腦網路危機處理暨協調中心（TWCERT/CC）會員，該中心可提供資安事件諮詢及協調服務,公司可有效接收及傳遞資安情資，達橫向資安聯防目標，共同維護網路安全，提升整體資安防護能量。

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，進行各系統帳號刪除作業。

3.落實資安訓練：

(1)為提高同仁資訊安全風險意識，不定期使用 E-Mail 宣導郵件社交攻擊態樣，並不定時進行社交工程詐騙。

(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。

(3)集團資訊安全教育宣導課程。

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)建置硬體虛擬化系統，提高系統可用度與容錯性。

(2)建置備份管理系統，定期『離線備份』將工作日星期一至星期五備份資料一份保留在機房，定期『異地備份』將每日備份的資料一份存放於異地（台中分公司機房），互相備援。

(3)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。

四、資訊系統損害對公司業務之影響與因應措施：

目前集團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。

五、114 年度「資通安全風險管理執行情形」，內容如下：

1.公司內部稽核

114 年 2 月 11 日～25 日稽核單位查核「系統復原計劃制度及測試程序之控制」及「資通安全管理作業之控制」，尚無發現異常或缺失事項。

2.郵件威脅統計

目前公司針對郵件的部份有安裝垃圾郵件管控機制來過濾並攔截惡意或廣告的信件。

3.防毒攔截

公司內的電腦皆有安裝防毒軟體，防止電腦中毒及電腦病毒的擴散。

4.年度資安事件

時間	資安事件	處置方式
114/01	微軟作業系統版本更新	114/01/01 起 114/12/31 止將新安裝電腦版本更新為 WINDOWS 11 Ver.24H2
114/10	防毒軟體版本更新為	版本更新至 12.12057.3
114/06 及 114/12	個人電腦登入密碼變更	大小寫英文+數字，長度為六碼以上

5.投入資通安全管理之資源

(1)由專業資安廠商協助防火牆連線規則備份與管理諮詢、防毒與備份系統授權與管理諮詢，並提供進階整合型端點防護.....等服務，每

年費用支出新台幣 115,500 元。

(2)114 年 12 月集團續約企業防火牆 Check Point QUANTUM（新台幣 80,000 元），加強內外網路防禦力此項專案建置提供多種安全模組及沙箱演練，其防護力較原舊有設備先進及安全。

(3)資訊主管於 114 年 6 月 4 日參加中小企業網路大學校線上學習平台【AI 人工智慧基礎介紹】56 分鐘線上課程。

(4)資訊主管於 114 年 6 月 5 日參加中小企業網路大學校線上學習平台【企業資訊安全認知（一）】37 分鐘時線上課程。

(5)資訊主管於 114 年 6 月 6 日參加中小企業網路大學校線上學習平台【企業資訊安全認知（二）】63 分鐘線上課程。

(6)資訊主管於 114 年 7 月 12、19 日參加中華民國資訊軟體協會【iPAS－中級資訊安全工程師－能力研習衝刺班】12 小時線上課程。

(7)資訊主管於 114 年 8 月 7 日通過 e 等公務員學習平台【114 個人資料管理通識課程】3 小時線上課程。

(8)資訊主管於 114 年 8 月 11 日通過 e 等公務員學習平台【資訊安全現況及挑戰】1 小時線上課程。

(9)資訊主管於 114 年 8 月 26 日通過 e 等公務員學習平台【114 年資訊安全教育訓練（一般人員）】3 小時線上課程。

(10)資訊主管於 114 年 8 月 28 日通過 e 等公務員學習平台【114 年資訊安全教育訓練（主管人員）】3 小時線上課程。

(11)資訊人員於 114 年 6 月 4 日通過中小企業網路大學校線上學習平台【人工智慧基礎介紹】56 分鐘線上課程。

(12)資訊人員於 114 年 6 月 26 日通過中小企業網路大學校線上學習平台【電腦網路與 OSI 參考模型基礎介紹】41 分鐘線上課程。

(13)資訊人員於 114 年 6 月 26 日通過中小企業網路大學校線上學習平台【企業資訊安全認知（一）】37 分鐘線上課程。

(14)資訊人員於 114 年 6 月 26 日通過中小企業網路大學校線上學習平台【生成式 AI 面臨法規之產業因應實務法律】74 分鐘線上課程。

(15)資訊人員於 114 年 7 月 25 日取得經濟部【資訊安全工程師－初級能力鑑定】之能力鑑定證書。

6.緊急應變暨系統復原計劃作業程序：

(1)資訊室於 114 年 5 月 20 日，依照「緊急應變暨系統復原計劃作業程序」執行系統資料災難復原演練。

(2)復原作業完成後移除網路並重新開機，確認復原電腦可使用帳號密碼登入，檢察系統服務有正常運作。

(3)請單位使用者操作檢查資料是否無誤。

7.參與集團資安宣導：電子郵件社交工程演練，分享最新社交工程攻擊手法與防範措施

(1)集團資訊室於 114 年 2 月 3 日至 12 月 15 日期間，透過電子郵件方式共發送 16 封資訊安全宣導信件，加強同仁資安意識。

(2)集團於 114 年 7 月實施「無預警電子郵件社交工程攻擊演練」。演練結果顯示，同仁整體資安警覺性已有明顯提升，惟仍有少部分同仁因誤判而點選假釣魚郵件。針對此次演練結果，集團於 114 年 8 月 4 日再次以電子郵件方式，檢附資安宣導短片及防範說明，提醒同仁務必提高資安警覺，切勿任意開啟不明來源之電子郵件，亦不得點閱郵件內之連結或附件，以避免遭受社交工程攻擊。

六、114 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。