資通安全風險管理執行情形

1.資通安全風險管理架構

本公司由隸屬於董事長之【資訊安全室】負責統籌制訂並定期檢討資安政策，建立資安事件通報與應變機制，持續深化防衛能力及加強同仁資訊安全意識並訂定電腦化資訊系統處理及控制作業，落實內控制度與維護資訊安全，透過每年檢視及評估其安全規章及程序，確保其適當性和有效性。每年至少兩次向董事長報告資訊安全執行情形與規劃且由稽核室每年就控制作業，進行資訊安全查核，評估公司資訊作業內部控制之風險改善。

2.資通安全政策

為落實資安管理，以期望達成下列政策目標：

(1).參考國際資安標準並遵守國內外資訊安全法規，定期修訂資訊安全規範。

(2).強化資安專業能力並與外部資安專家團隊合作，早期發現並防止資安威脅。

(3).確保資訊資產之機密性、完整性。

(4).控制各部門資料存取權限，防止未經授權之資料修改或系統存取。

(5).持續資安教育宣導及災難復原演練。

(6).不定期進行釣魚郵件演練及防範措施。

(7).每季進行資安會議討論及防範措施。

3.具體管理方案及投入資通安全管理之資源

(1).網路攻擊防禦：建置新世代防火牆與入侵偵測系統防止系統被惡意攻擊或入侵。

(2).防毒防駭防勒索：電腦設備佈建完整端點防護軟體並定期修補。

(3).郵件閘道主機：建置電腦病毒與惡意軟體過濾機制。

(4).電腦設備定期更新安全修補檔案：電腦系統自行派送安全修補檔案以防止安全漏洞產生。

(5).OA 系統主機虛擬化:OA 重要系統主機皆虛擬化並定期備份，若有主機故障可迅速移轉復原。

(6).RD 研發資料不落地:公司重要 RD 研發技術皆在 Citrix 環

境內開發，可避免資料外洩，或被惡意攻擊的風險並定期備份。

(7).電腦機房不斷電系統：機房內所有設備皆接在不斷電系統上，以確保電源穩定並由廠商保養維護。

(8).資料存取記錄備存：系統與文件皆定期備份並每年不定期執行系統資料復原測試，以確保資訊系統之正常運作及資料保全完整。

(9).資訊部門軟硬體設備的資產需統一管理，並有效的保護資產。

(10).確保資訊帳戶存取權限與系統之變更，均經過公司規定程序授權處理。

(11).監控資訊系統之安全，有效掌握並處理資訊安全異常事件。

(12).已加入 TWCERT/CC 和科學園區資安資訊聯盟以取得最新資安情資。

(13).自 113 年 1 月起每季定期召開資安管理會議,制訂與調整資訊安全政策,審查資訊安全發展現況及未來方向,確保資訊安全管理制度持續運作。

4.投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

(1).專責人力：設有專職之企業組織「資訊安全室」負責公司資訊安全規劃、技術導入與相關的稽核事項，以維護及持續強化資訊安全。

(2).資安公告：本年度發佈 2 份資安中心公告，傳達資安防護相關規定與注意事項。

(3).所有新進員工於新人教育訓練時，進行資安政策及目標之宣導。

(4).不定期跟同仁宣導資安風險及目前最新的資安情資，以強化人員資安意識。

(5).本年度指派資訊安全室同仁參加 4 次外部資通會議及資通安全教育訓練課程，吸收新知更新資安知識。

(6).客戶滿意：無重大資安事件，無違反客戶資料遺失之投訴案件。