資通安全管理

有關本公司資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等說明如下：

1.資通安全風險管理架構：

(1)設置資安專責主管及一名資安專責人員，負責資訊安全政策管理與規劃，並負責資訊安全相關事件處理與通報。

(2)針對資訊安全之防毒、防災、防駭、防漏等之機制，定期向資安專責主管進行彙整報告。

2.資通安全政策：

訂定資訊安全政策暨管理辦法，確保本公司資訊資產之機密與安全及法律遵循，以期資安問題發生時，對營業之影響降至最低。

3.具體管理方案：

(1)端點設備保護與控制：

安裝防毒軟體、保持作業系統更新、並以網域控管相關存取限制。

(2)中央對外控制：

對外部網路存取使用集中式威脅管理設備(UTM)管理、郵件伺服器提升為微軟雲端伺服器、反向代理(Reverse Proxy)伺服器建置，及相關子系統登入機制漸次提升為雙重要素驗證(2FA)。

(3)資料保護：

透過先進檔案系統對重要資料進行高頻率之多層次(Multi-tier)與異地(off-site)備份，持續進行資料保護。

(4)資安宣導：

針對同仁定期進行資訊安全宣導，加強資安意識、強化資訊安全防護。

4.資通安全管理資源：

●執行結果

(1) 定期資安會議：

開會日期	開會主題
6/10	MDR 導入規劃
6/17	OETH 雲端身分驗證導入規劃

(2) 定期報告董事會:

本公司於第六屆第十五次董事會(2024.12.27)彙報資安管理、資安相關議題及資安風險評估等事宜。

(3) 定期宣導資安議題：

日期	資安宣導內容
4/8	第一次社交工程演練
5/14	總部員工資安教育訓練
5/21	第二次社交工程演練
6/3	資安宣導-妥善保管個人帳號密碼

(4) 2024 年投入資安之總經費：

日期	項目	金額
4/24	異地機房費用	114,030
11/5	營運主機硬體維護費	113,505
12/1	導入 MDR	300,000
12/1	導入 OETH 雲端身分驗證	300,000