中傑集團
Chung Jye Group

中傑集團資通安全管理運作情形

● 資通安全風險管理架構

1. 成立資通安全推動組織，配置適當的人力、物力和財力資源。
2. 指派合適的人員擔任資安專責主管和資安專責人員，負責推動、協調監督和審查資通安全管理事項。
3. 制定資通安全政策、目標和作業程序，包括核心業務、資通系統盤點、風險評估、防護措施、事件應變等。

● 資通安全政策

1. 鑑別公司的核心業務和敏感性資料。制定核心業務持續運作計畫，進行災害還原演練和持續改進。
2. 定期盤點資通系統，建立核心系統資產清單，進行資安風險評估，分析可能的風險，採取相應的管理和技術控制措施。
3. 區隔不同作業環境，建立防火牆、防毒、入侵偵測等控制措施。對敏感性資料進行適當的保護，採取加密、存取控制措施。定期進行弱點掃描和滲透測試。

● 具體管理方案及投入資通安全管理之資源

1. 訂立 Internet 使用規範，配置防火牆 (WAF)防範。
2. 建置入侵預防系統(IPS) 資安設備防護。
3. 部署防毒系統、郵件安全閘道、網頁代理系統 (Web Proxy) 。
4. 電腦安裝端點偵測與回應系統 (EDR)。
5. 設有資安監控中心(SOC)以進行 7 x 24 不間斷之資安監控與回應。
6. 訂定密碼管理制度，並啟用 2FA 認證機制。
7. 入職調職離職，帳號權限控管機制。
8. 訂立核心業務軟體修改版本控制制度。
9. 設置完整備份規劃，包含本地、異地、雲端備份機制。
10. 訂定資安事件應變處置和通報作業程序，成立資通安全事件通報及應變小組，並在平時進行演練。
11. 資通系統或資通服務委外管理，建立委外廠商的資安責任和保密規定。

- **針對資通安全管理，相關的執行情形**

1. 設置資安主管一人、資安執行小組三人、資安緊急處理小組三人。資訊人員每年至少接受 8 小時以上，以及資訊安全專責單位人員每年至少接受 15 小時以上資訊安全專業訓練。
2. 實施全公司台灣、中國、越南一般人員 3 小時資安訓練。
3. 2024 第二季執行社交工程釣魚郵件演練，共發出全集團 921 封 偽裝釣魚信件，共有 7.71%點擊連結，1.19%點擊連結後輸入資料。對點擊人員進行資安教育訓練，並進行考試審核。
4. 加入 TWCERT 資安情資分享組織，取得資安預警情資。
5. 2024 年指派一人參加 ISO27001 資安稽核員認證。
6. 實施台灣與中國區域 ERP 系統完整災害備份還原演練