

# 資通安全治理暨風險評估報告(2024)

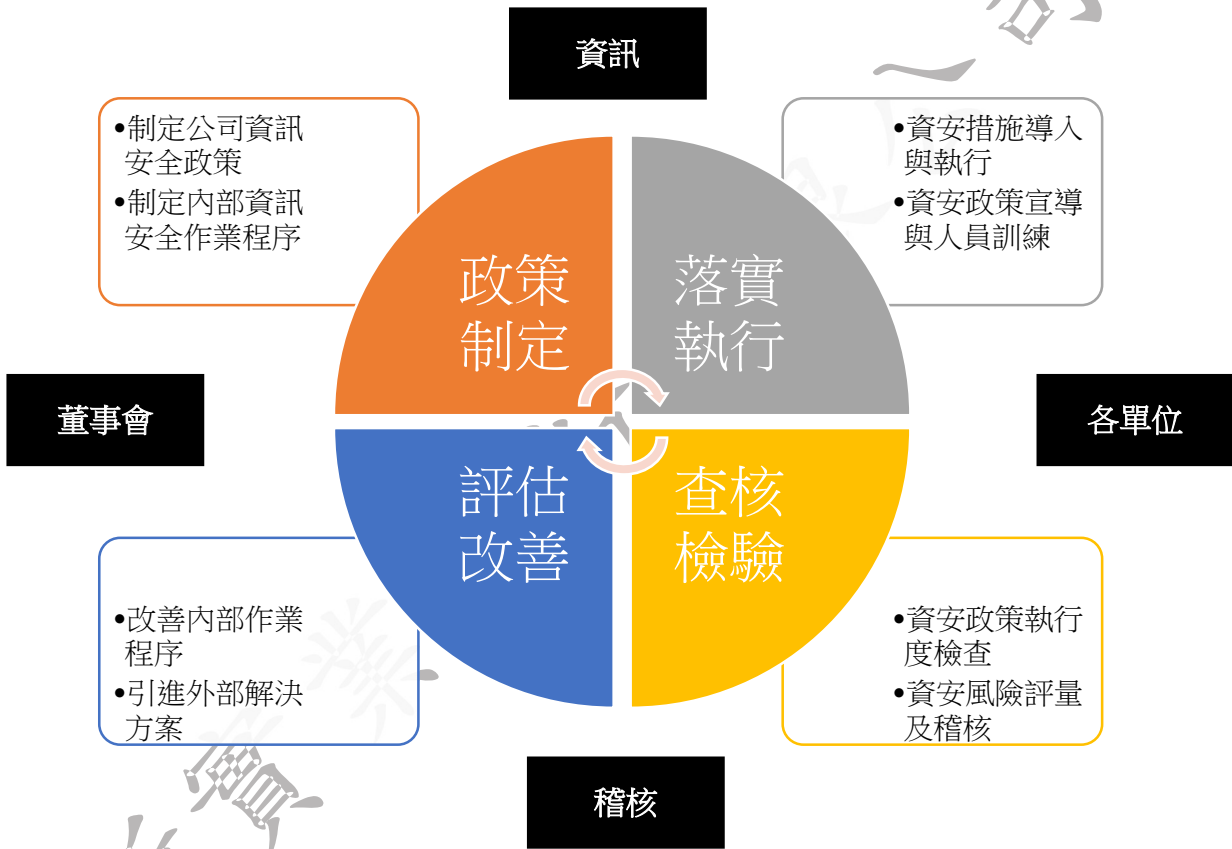
<摘要版>

## 一、資通安全管理策略與架構

本公司為配合國家資通安全政策、強化公司內部資訊安全管理，以確保所屬之資訊資產的機密性、完整性及可用性之資訊環境，並符合相關法規之要求，制定相關資安管理辦法規範。

### 1-1. 資通安全風險管理架構

本公司資安及稽核人員每年定期自評及查核資訊安全相關作業，若過程發現缺失，即檢討、要求提出改善措施，追蹤改善結果，以降低內部資安風險。資訊安全管理策略採用 PDCA (Plan-Do-Check-Action) 循環流程管理模式，確保可靠度目標之達成且持續改善。



### 1-2. 資通安全政策

本公司資訊安全政策，包含制度規範、科技運用、人員訓練三個面向：

- 1-2-1. 制度規範：訂定公司資訊安全管理制度，規範人員作業行為。
- 1-2-2. 科技運用：建置資訊安全管理設備，落實資安管理措施。
- 1-2-3. 人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。

### 1-3. 具體管理方案

- 1-3-1. 制度規範：本公司訂有資安管理辦法及多項控管措施，以規範本公司人員資訊作業行為，並定期執行內部稽核及資安自評，並由會計師進行資訊、資安查核，以檢視相關規定是否符合營運環境變遷，依需求適時調整。
- 1-3-2. 科技運用：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更使用中

華電信資安艦隊的多項服務，以提昇整體資訊環境之安全性。

1-3-3. 人員訓練：本公司定期實施員工的資訊安全教育訓練課程，資訊人員持續參加資安研討會或外部課程，藉以提昇本公司人員資安知識與專業技能。

#### 1-4. 投入資通安全管理之資源

本公司每季以時事案例做為資通安全宣導，為加強資訊安全，民國 113 年已編列預算強化資訊安全防護，且每年定期向董事會報告資通安全管理及執行成果。

## 二、資通安全管控及治理

### 2-1. 資安管理之重點策略

2-1-1. 管制作業權限：人員資訊作業之權責劃分與審核、權限帳號定期盤查與複核。

2-1-2. 落實存取控管：File Server 的帳號管控存取、資料傳輸的管道控管，密碼混合編碼及定期變更要求。

2-1-3. 阻隔外部威脅：中華電信資安艦隊的 UTM 防火牆端點防護、防駭守門員企業版及入侵防護服務。

2-1-4. 強化系統可用性：使用 NAS 資料備份及異地備援措施、定期災害還原演練。

### 2-2. 重大資通安全事件

截至年報刊印日止，無發生重大資通安全事件導致任何損失及影響。

以下為本公司資安事件等級說明：重大資安事件為第二、三級。

等級	說明	影響範圍	通知層級
第一級	單獨電腦	個人電腦、資料	資安窗口→資安主管、單位主管
第二級	辦公室區域	個人電腦、資料、	資安窗口→資安主管、
第三級	全公司	伺服器、網路設備、資料庫	部門主管→總經理

### 2-3. 資通安全風險管控措施

本公司對資安風險之管控以內部控制為基礎，參考外部實例或廠商建議而持續改進，所採取之管控措施(如下表)乃衡量經營管理階層對營運宗旨與企業價值之共識，針對核心業務及重要工作之發展進程，依 ISACA 國際電腦稽核協會台灣分會之"資通安全公司自我檢查表"的 10 個分類，每年定期自我評估及分析後，依據其中風險性較高的部份進行檢討及擬具改善措施，從系統面、技術面、程序面，對已知之威脅採取適當之處理方法，對潛藏之威脅盡可能予以事前分析及鑑別，以保護公司資訊財產的機密性、可用性及完整性，避免遭受各種威脅及降低可能的危害或損失，以提升本公司承受外部攻擊之防護能力及應變彈性，減緩衝擊等級及降低可能造成的損害，妥善因應風險。

項次	資安管理分類	重要管控及防護措施	執行頻率
1	資訊安全政策	1.明定資安組織、權責及事件之通報、處理綱要。 2.定期審查、修訂資訊安全政策。	檢視 1 次/年
2	建立資訊安全組織	1.設資安管理小組及個人資料保護小組。 2.訂立資安事件之緊急應變處理及回報程序。	年 不定期
3	人員安全與管理	1.內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。 2.每半年執行作業權限複核。 3.每年定期普查個人電腦，防止公器私用。	檢視 1 次/年 半年 年
4	資產分類與控管	1.資訊類軟、硬體資產列冊管理。 2.每年定期普查電腦，確認軟、硬體資產。	年 年
5	實體及環境安全管理	1.專用電腦機房具溫度、電力自動控管。 2.伺服器及個人電腦安裝防毒軟體，重要職務之電腦，每日定時備份，其備份份數至少二代。 3.異地備份機制。	日 日 週
6	通訊與操作管理	1.電子郵件主機具自我防護及保存稽核之功能。 2.每日分析防火牆紀錄，並使用趨勢雲端防毒防駭軟體分析、記錄上網行為，即時防堵內、外部異常行為。 3.即時宣導資安事件、通告或案例，提升防護意識。 4.使用 Hinet 資安艦隊之防駭守門員、先進網路防禦等服務，擴展防禦的廣、深度，防堵內、外之攻擊。	週 日 季 週
7	存取控制	1.電子檔資料依部門、個人設定存取權限。 2.對外連線作業申請需經透過電話或 mail 通知。 3.電子郵件區分權限，不須對外連絡者僅能內部寄信。 4.人力資源系統於讀取個資時，自動記錄存取軌跡。	不定期 不定期 需申請 不定期
8	系統開發與維護	應用系統為套裝軟體，委外開發、維護，在更新程式及系統時，限制連線方式及時間，防範外部的侵入篡改。	不定期
9	永續運作之計畫管理	1.營運資料庫定期模擬事故演練、測試。 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。	季 需要時執行
10	內部稽查及其它	1.每年電腦普查時告知公司軟體所授權之範圍，規範以外之軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 2.資訊單位每年定期自評資訊作業環境安全。 3.內部稽核人員及會計師每年定期稽查資訊控制作業。	年 年 年

資訊單位於 2024 年 12 月對上列管控措施在執行上的達成度或完整度進行評量，共分為五級的成熟度：完整、良好、尚可、待加強、差，自評結果為” 尚可” ，自評報告經資安主管及總經理核閱，並依據風險性較高的部份進行檢討及擬具改善措施

### 三、結論

從本次資安治理風險評估之 3-3-2.資產類別風險分布表中觀察，平均風險指數約五成，呈現外部威脅已是常態性，而公司整體風險有八成是在低範圍內，表示本公司資安環境仍保持穩定，現有的內部控制和管理措施，對於風險的識別與應對，發揮了重要作用，有效減少了潛在的安全事件發生概率。因此，儘管面對部分無法預知的潛藏威脅，內部系統的運作仍處於可控範圍內，針對威脅及風險值偏高的部分，未來還有提升改善的空間。

針對中風險等級項目偏多的電腦系統及軟體，將確保作業系統及各項應用程式的即時更新，避免已知漏洞導致損害、產生安全風險，並定期進行系統性能優化，確保各系統運行的穩定性與效能；對營運相關之資訊系統及資料庫的智慧財產，應持續加強資料存取控制及評估導入加密機制，並確保資料庫日誌的完整性和可追蹤性。

隨著資安威脅形勢的不斷演變，新的年度本公司將持續推動內部控制及管理的優化，著重於強化風險預警機制和應急響應流程，確保資訊安全政策能夠進一步落實。這將包括加強員工教育訓練、優化資安防護技術、提升對新興威脅的防禦能力，並定期進行風險回顧與評估。我們有信心，通過不斷改進和完善資安管理體系，能夠有效應對未來可能出現的各種風險挑戰，保障公司資訊安全及業務穩定運行。

製作單位及日期	資安管理小組 2025/2/10
呈報董事會日期	2025/3/11