資訊安全政策

為強化本公司資訊及通訊安全防護與管理機制，確保資訊資產的**機密性、完整性及可用性**，天能綠電股份有限公司特訂定本政策，以建立穩健的資訊安全管理架構，防止內外部威脅，確保業務運作安全與永續。

本政策適用於本公司所有資訊資產、資訊系統及相關作業活動，包含公司內部員工、委外廠商、合作夥伴、訪客及任何以電子方式存取或處理資訊之人員，皆應遵守本政策規範。

一、資訊安全管理原則

本公司依據國際資訊安全管理精神，依循「**辨識、防禦、偵測、應變、復原、訓練**」六大面向推動資安措施：

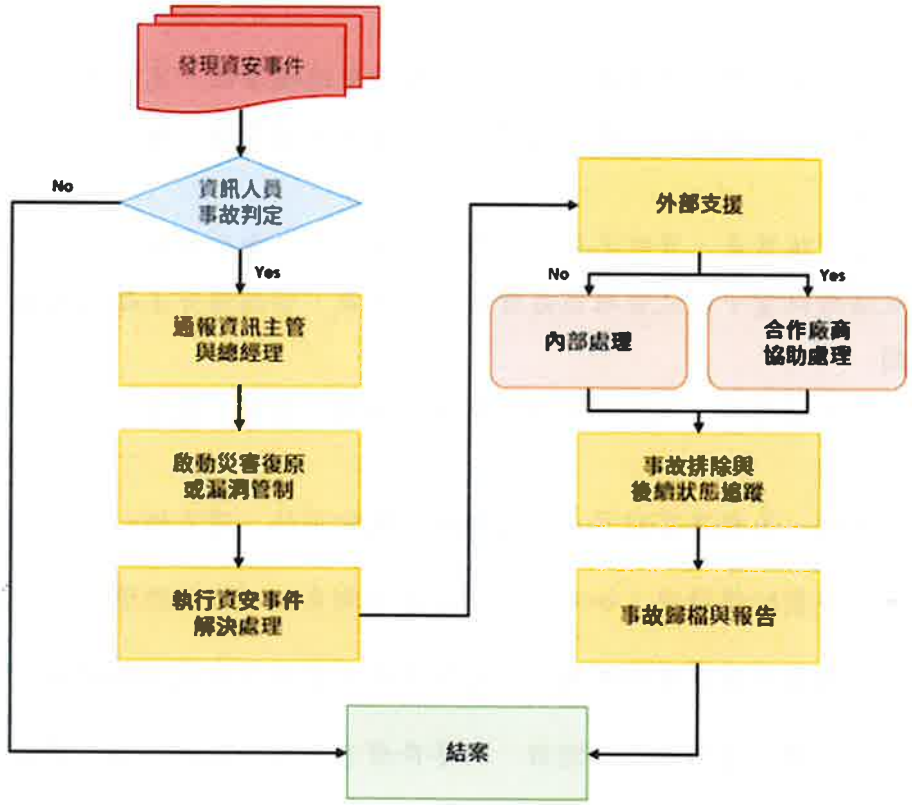
1. **辨識**：掌握關鍵業務、系統及資訊資產，定期執行風險評估，建立核心資產清冊。
2. **防禦**：依風險等級規劃防護措施，如防火牆、入侵偵測系統、權限控管及資料加密。
3. **偵測**：建置異常行為與網路威脅偵測機制，定期更新病毒碼與系統弱點掃描。
4. **應變**：建立資訊安全事件通報與應變流程，於事件發生時即時啟動通報、調查與修復。
5. **復原**：設置備份與備援計畫，確保營運於最短時間內恢復正常。
6. **訓練**：定期舉辦資安教育與社交工程演練，提升員工安全意識與應變能力。

二、資通安全管理

- 訂定並定期檢視資訊安全政策、目標及作業程序。
- 監督核心資通系統與關鍵資料之風險評估與防護。
- 確保委外廠商符合資安要求，訂有保密及責任條款。
- 定期向管理階層或董事會報告資訊安全執行情形。
- 定期辦理內部及外部資安稽核與教育訓練，持續精進管理績效。

三、資訊安全事件通報程序

當發現資訊安全事件時，資訊人員應立即進行事故判定。若確認為資安事件，須依下列程序處理



四、責任與懲處

所有員工及委外人員皆有維護資訊安全之責，若發現異常應立即通報。對於因疏失、違規或故意行為導致資安事件者，本公司將依情節輕重追究民事、刑事及行政責任，並依內部規章辦理懲處。

五、審查與改善

本政策每年至少檢討一次，並依科技發展、法令變更及公司營運需要進行修訂，以確保政策持續適用與有效。所有修訂均應經永續發展委員會及董事會決議通過後公告施行。

董事長　　總經理