群光電能科技（股）公司
資訊安全風險管理暨執行情形

目錄

一、 資通安全目的與範圍

對象：包括員工，客戶，供應商以及營運相關資訊設備及資料。

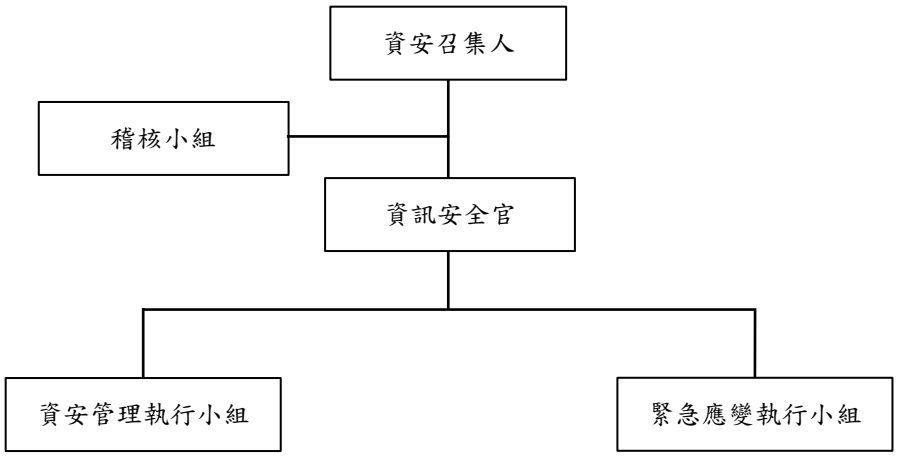
範圍：為確保本公司資訊安全，制定相關規章制度，應用技術和數據安全標準制定，並

納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

二、 資通安全組織架構

1. 為落實本公司資訊安全管理之標準化政策，特設置「資訊安全管理委員會」以推動相關工作事宜，由本公司資訊處最高主管擔任資安召集人，資訊處負責主導及規劃，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
2. 本委員會負責制定資訊安全管理政策，定期檢討修正。
3. 本委員會定期召開會議檢討執行情形，並每年定期向總經理報告執行情形與檢討。

「資訊安全管理委員會」組織架構：



三、 資通安全政策

1. 建置資訊安全管理制度並持續改善。
2. 提供相關必要資源，適當分配權責。
3. 確保本公司資訊之機密性、完整性及可用性。
4. 遵守法令法規。

四、 資通安全目標

本公司為保護重要資訊、提升服務品質、確保資安政策可有效達成，特訂定以下資安目標：

1. 維持資訊安全管理系統有效性。
2. 確保資訊資產之安全性、完整性與正確性。
3. 保障資訊安全管理資源充足。
4. 關鍵業務持續運作。
5. 確實遵循法令法規。

五、 資通安全管理作為

1. 本公司所有同仁、委外廠商暨其協力廠商須簽定保密聲明書，已確保使用本公司資訊以提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。
2. 公司定期執行資訊安全宣導作業，每季定期發布資訊安全相關公告，加強公司同仁資訊安全宣觀念，且每位同仁須簽定資訊保密協定。
3. 公司同仁對於帳號、密碼與權限應善盡保管與使用責任並定期換置，且須遵守法律規範與資訊安全政策要求，主管人員應督導資訊安全遵行制度落實情況，強化同仁資訊安全認知及法令觀念。
4. 建立及定期盤點資訊資產清單，依風險評鑑進行風險管理，落實各項管控措施並制定資訊安全

事件的回應及通報標準程序，以適當對資訊安全事件做即時處理。

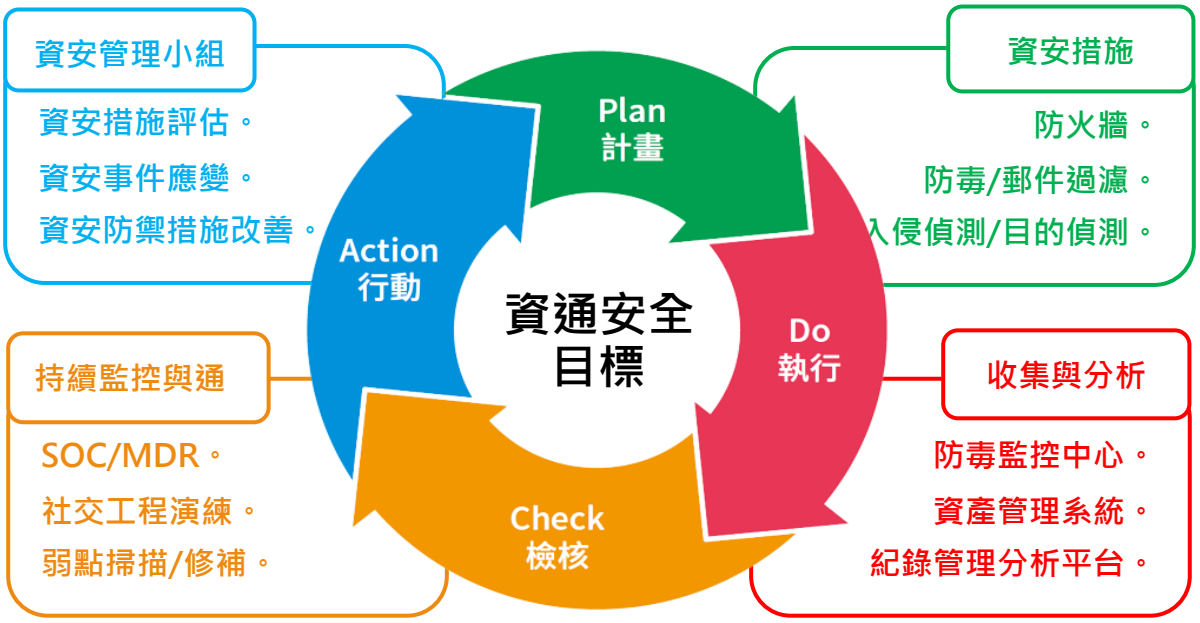
5. 對於資安事件應變及預防，本公司針對重要資訊系統已導入從網路邊界到電腦終端的資安防禦系統，並建置適當之備援或監控機制並定期演練，維持其可用性。。
6. 為提升應用系統安全與降低風險，每年定期執行弱點掃描並對中高風險的弱點進行修補，並已導入MDR託管式偵測及回應服務，降低異常事件的發生。
7. 針對電子郵件導入BEC、APT防護模組進行過濾，持續強化資通安全管理機制。
8. 本公司亦委外專業資安廠商，每日不間斷監控資安事件，如遇資安事件發生，即可即時處理，避免傷害擴大。
9. 公司同仁使用電腦一律安裝防毒軟體且定期確認病毒碼之更新，並禁止安裝未經授權軟體；且硬體更換及軟體安裝，一律由資訊處同仁處理，避免有資訊安全疑慮。。
10. 公司同仁禁止攜帶私人電腦至公司使用，以防私人行為造成公司不當影響。

六、 資通安全目標及達成狀況

為了在既有良好的資安管理基礎上，能持續確保客戶隱私與機密資訊之安全，本公司已於 2023 年導入「ISO 27001：2013」資訊安全管理系統，訂定資通安全政策及相關四階管理文件，並定期取得 ISO 27001 認證。

目前已取得之證書有效迄日為 2025年 10月 31日，並持續採取 PDCA 方法，改善整體資通安全的環境，建立可量測的資通安全目標，定期檢視和評估目標達成的狀況。透過每年定期的內部稽核、 ISO 27001 資訊安全管理系統審查以及會計師電腦審計，強化資訊安全事件之應變處理能力，保護公司與客戶之資產安全。

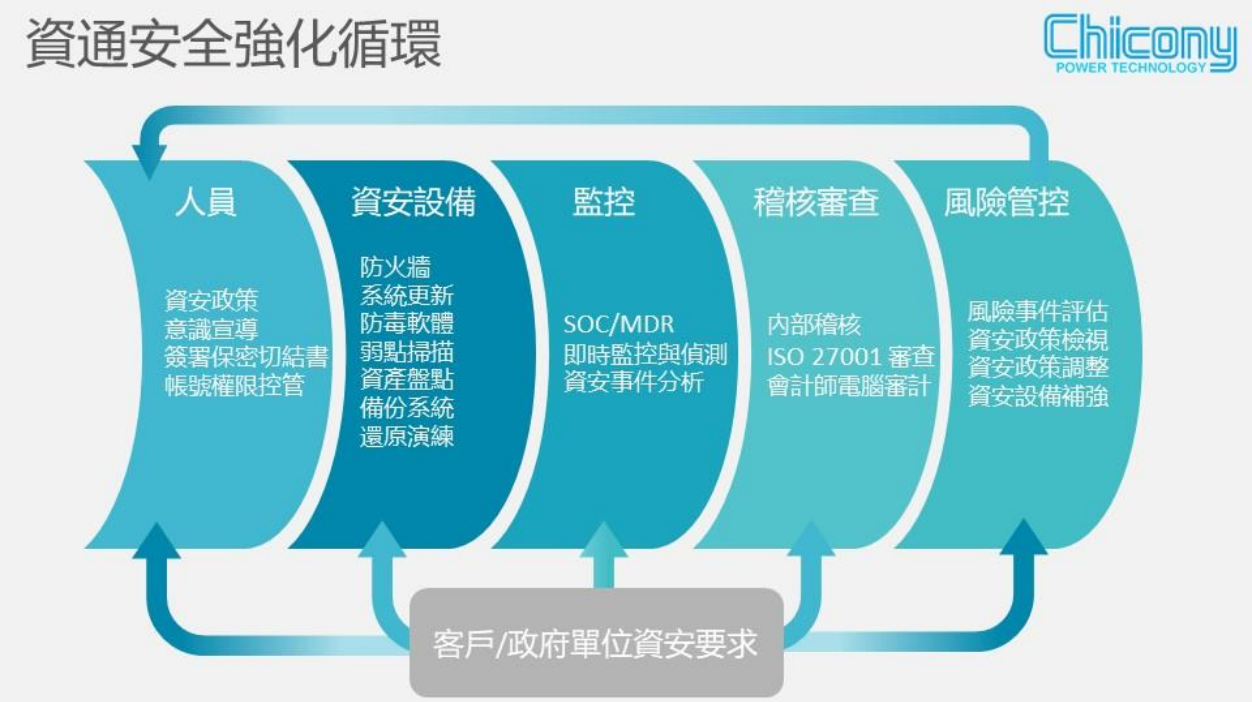
PDCA 方法：



資通安全目標：

本公司亦經由外部資安機構定期執行資安風險檢視，並結合資安威脅情資，調整資安政策，更新系統，以及資安設備的設定，以降低資安風險。

經由上述資通安全強化的循環，以及符合客戶/政府單位的資安要求，不斷強化本公司的資訊安全。



七、 資訊安全與客戶隱私之管理架構

保護機密資訊與客戶隱私是客戶多年來與本公司維持建立合作關係的原因之一，公司為維護客戶的權益將致力於保護客戶資訊安全，並視為本公司最重要的資通安全管理目標，與客戶建立長久互信之合作關係。

八、 資訊安全之風險

本公司依照「上市上櫃公司資通安全管控指引」以及 ISO 27001 的標準，已建立一套完整的資訊安全管理制度，並依照其制度建置符合公司需求的資訊系統及資訊安全設備。經由每年檢視各項規章和程序，評估資訊安全風險，以確保其制度的有效性，但仍有可能會受到不斷變化的資安風險所影響。

九、 辦理資通安全宣導執行情形

每季定期公告並視情況不定期宣導。本公司已訂定「風險管理政策與程序」，並將資訊安全相關風險狀況及執行情形提報 2024年 董事會。

2024年度 截至 9月 30日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無。