

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
- 二、 資通安全組織架構
- 三、 資通安全政策
- 四、 資通安全目標
- 五、 資通安全管理作為
- 六、 資通安全目標及達成狀況
- 七、 資訊安全和客戶隱私之管理架構
- 八、 資訊安全之風險
- 九、 辦理資通安全宣導執行情形

一、資通安全目的與範圍

1. 適用對象

本政策適用於所有涉及本公司資訊資產之利害關係人與資訊環境，包括但不限於：

- I. 本公司全體員工（含臨時人員、實習生等）
- II. 客戶、合作夥伴及外部供應商
- III. 委外服務廠商及其協力單位
- IV. 本公司所有營運相關之資訊系統、網路設備、軟硬體設施、雲端平台及資料資源

所有涉及本公司資訊接觸、處理與傳輸之人員及單位，皆須遵守本政策，以確保資訊資產之安全與隱私。

2. 管理範圍

為全面落實資訊安全防護，本公司依循國際標準及法令規範，訂定相關規章制度，涵蓋下列範疇並納入日常管理運作體系：

- I. 資訊資產保護
針對所有資訊資產（包含數據、文件、系統、應用程式與設備）實施分級管理，確保資產在使用、儲存、傳輸及銷毀過程中均受到適當保護。
- II. 制度與技術控管
建立包含資訊安全政策、作業程序及行為規範之管理制度，並導入防火牆、入侵偵測、防毒系統、加密技術等安全機制，以降低營運風險。
- III. 隱私與個資保護
遵循個人資料保護法及國際隱私規範，確保員工、供應商及客戶於進行業務往來、資訊處理或資料交換時，其隱私權與個人敏感資訊均獲得妥善保護。
- IV. 持續營運與風險管理
將資訊安全管理制度與公司營運緊密結合，透過定期稽核、教育訓練及持續改善機制，確保公司能有效因應資訊風險與突發事件，維持業務營運之穩定性與連續性。
- V. 合作夥伴責任
對所有供應商及委外合作廠商，要求其遵循相同之資訊安全規範，並透過契約義務與監督機制來確保其遵循度，以強化整體資安防護鏈。

二、資通安全組織架構

1. 委員會設置與職責

為落實本公司資訊安全管理之標準化政策，並確保資訊安全治理架構有效運作，本公司特設立「資訊安全管理委員會」作為最高層級之資安推動組織。由資訊處最高主管擔任資安召集人，統籌規劃與督導資安相關工作；資訊處負責政策制定、制度規劃及執行推動；各業務單位依其職能範疇配合執行，確保跨部門協作，以全面強化本公司資訊安全管理效能。

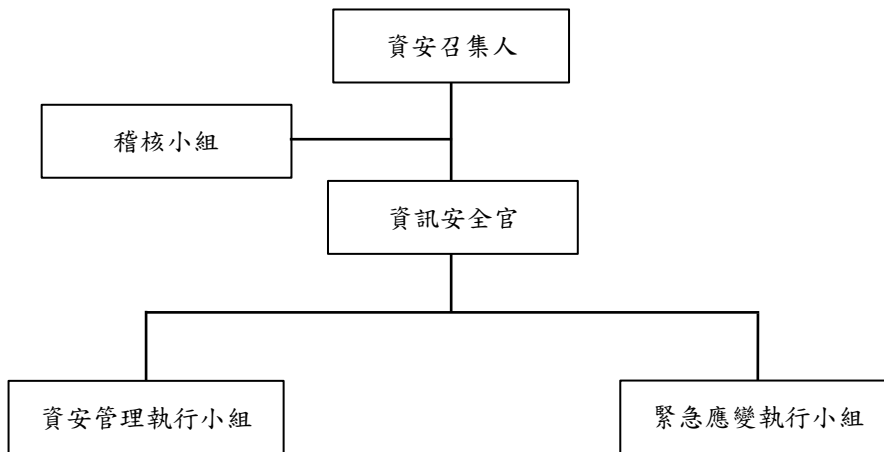
2. 政策制定與持續改善

本委員會負責研擬與制定本公司之資訊安全管理政策、目標及相關規範，並依據內外部環境變化、法令更新及技術風險狀況，進行定期檢視與修正。透過持續改善之機制，確保資訊安全政策能長期符合公司營運需求及國際標準要求。

3. 會議運作與執行追蹤

本委員會每季定期召開會議，檢討資訊安全措施之執行情況，並針對重大資安議題或資安事件召開臨時會議進行因應，以確保即時決策與處置效能。同時，委員會須每年定期將整體執行成果、風險評估報告及改善計畫，完整呈報予總經理進行審視與指導，以確保公司資訊安全治理落實於管理核心。

4. 「資訊安全管理委員會」組織架構：



三、資通安全政策

1. 建置並持續完善資訊安全管理制度

本公司致力於依循國際標準(如 ISO 27001)建置完善之資訊安全管理制度，並透過定期檢討與內外部稽核，持續改進現有流程與防護措施，確保管理制度與時俱進，能有效因應新興威脅與快速變化的資訊環境。

2. 提供必要資源並適當分配權責

為落實資安政策，本公司承諾提供足夠且適切之人力、財務與技術資源，並明確界定各部門及人員之資訊安全責任與權限，確保所有防護措施與應變機制能有效實施，以提升組織整體防禦與應變能力。

3. 確保資訊之機密性、完整性與可用性

為維護資訊資產安全，本公司將持續透過存取管控、加密技術、稽核監控以及備援機制，確保資訊在傳輸、處理與保存過程中，維持最高水準之機密性、完整性與可用性，以保障公司營運與客戶權益。

4. 嚴格遵循法令及國際規範

本公司承諾遵循國內外相關法律、政府規範以及契約義務，並持續監測法規趨勢，確保資訊安全政策及各項作業流程能符合法令要求。透過內部稽核與持續監督，確保合規性之落實，並維護公司聲譽與客戶信任。

四、資通安全目標

本公司基於「保護重要資訊資產、提升服務品質、確保資安政策有效落實」之原則，依循國際標準及相關法令規範，特訂定以下資訊安全目標，以作為全體同仁及相關合作夥伴共同遵循之方向：

1. 維持資訊安全管理系統之有效性

本公司承諾持續導入並完善符合國際標準之資訊安全管理系統(ISMS)，透過PDCA 管理循環以及內外部稽核機制，確保制度能長期有效運作與持續改善，維持最佳防護能力。

2. 確保資訊資產之安全性、完整性與正確性

本公司將持續建置與優化資產盤點、權限管控及存取監控措施，避免未經授權使用與外洩風險，確保所有資訊資產能在運用過程中維持正確性與完整性，並支持公司營運及客戶服務之穩定性。

3. 保障資訊安全管理資源之充足性

為確保資訊安全政策能落實推動，本公司承諾提供充足且適切之人力、技術與財務資源，並持續培養員工的資安意識與專業能力，以提升整體防護效能及應變能力。

4. 確保關鍵業務持續運作

本公司透過建置備援系統、災難復原計畫(DRP)及營運持續計畫(BCP)，強化業務連續性管理，以降低重大資安事件或突發狀況對公司營運及客戶服務造成的影響，確保關鍵業務得以不間斷運行。

5. 確實遵循相關法令與規範

本公司承諾遵循國內外相關法令、政府規範及契約義務，並持續檢視法規遵循狀況。透過內部稽核與法規遵循審查，確保所有資安作業符合法規標準，同時維護本公司之信譽與客戶信任。

五、資通安全管理作為

1. 保密義務

本公司全體同仁、委外廠商及其協力廠商，均須簽署保密聲明書與相關協議，以確保於提供資訊服務或執行業務過程中，妥善保護所接觸或使用之本公司資訊資產。所有人員均有責任防範資訊遭未經授權存取、竄改、破壞或不當揭露，並應主動遵循本公司訂定之資訊保護措施。

2. 資訊安全宣導

為持續強化資訊安全文化，本公司定期推動資訊安全宣導與教育訓練，每季發布資安公告，提升全體同仁的資安意識與防護能力。同時，所有同仁均須簽署資訊保密協定，以明確承諾落實資訊安全責任，強化組織整體安全意識。

3. 帳號與權限管理

各同仁應妥善保管並正確使用個人帳號、密碼與系統權限，須定期更新，以降低帳號遭盜用之風險。所有操作須遵循資訊安全政策及相關法規規範。主管人員則負有監督職責，以確保權限管理制度落實，並透過定期檢視提升同仁法規遵循與資安警覺心。

4. 資訊資產管理與風險控管

公司定期建立與更新資訊資產清單，依據風險評估結果採取適當之風險管理措施，並制定配套控管方式。另亦健全資訊安全事件通報與處置流程，以利於發生突發狀況時，能即時且有序地回應，降低對營運及客戶權益之影響。

5. 資安防禦與演練

本公司於重要資訊系統全面導入多層次防禦機制，自網路邊界至終端設備皆設置資安防護，並建立備援及即時監控機制。除此之外，公司亦定期進行資安演練與模擬測試，以驗證防禦措施可行性，並確保系統可用性與營運持續性。

6. 弱點管理與事件偵測

本公司每年定期執行系統與應用程式弱點掃描，針對高風險以上的弱點立即進行修補與調整。同時，已導入 MDR(Managed Detection and Response)託管式偵測與回應服務，透過即時監控和專業分析，有效降低異常事件的發生率，提升威脅偵測與快速回應能力。

7. 電子郵件防護

為降低電子郵件相關威脅風險，本公司已導入 BEC(商務郵件詐騙防護)與 APT(進階持續性威脅防護)模組進行智慧化過濾，防堵詐騙與惡意攻擊。並透過持續優化過濾規則及教育訓練，協助同仁辨識可疑郵件，建立更嚴密的電子郵件安全管理機制。

8. 委外專業監控

除了內部資安防護機制之外，本公司並委託專業資安廠商提供 24 小時即時監控服務，確保能迅速發現並即時回應各類資安事件。藉由專業團隊的持續監測，可有效避免資安威脅擴大，確保營運穩定與客戶資訊安全。

9. 軟硬體管理

本公司規範全體同仁使用之電腦須安裝防毒軟體，並定期更新病毒碼，以確保能防範最新威脅。嚴禁安裝未經授權軟體，以避免惡意程式或未明風險進入公司網路。所有硬體更換及軟體安裝作業，由資訊處專責人員統一執行，以降低資安風險並提升資產管理效率。

10. 設備使用規範

為避免因私人行為造成資安風險，本公司規定嚴禁同仁攜帶或使用私人電腦於公司環境。此舉旨在降低外部裝置攜入惡意軟體或不當存取之風險，確保辦公環境與系統安全，保障公司營運及客戶資訊資產完整性。



六、資通安全目標及達成狀況

為持續確保客戶隱私及機密資訊安全，在既有良好資安管理基礎之上，本公司於2023年正式導入「ISO 27001:2013」資訊安全管理系統，並制定資通安全政策及四階管理文件，藉以強化治理架構，同時透過定期稽核以維持認證效力。

於2025年07月08日及2025年07月23日，本公司已分別完成「ISO 27001:2013」轉版至「ISO 27001:2022」之定期稽核與轉版驗證，並順利通過審查；「ISO 27001:2022」證書有效期限自2025年10月22日至2026年08月02日，原始註冊日期為2023年08月02日。

本公司將持續依循PDCA (Plan-Do-Check-Act) 循環管理方法，持續優化資通安全治理環境，並建立可量測之資通安全目標，定期檢視與評估其達成情況。同時，透過年度內部稽核、「ISO 27001:2022」管理系統審查以及會計師電腦查核，以強化資安事件之即時應變與風險控制能力，確保公司與客戶之資訊資產能獲得最高程度的安全保障。

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。

PDCA (Plan-Do-Check-Act) 循環管理方法：



可量測之資通安全目標：



資通安全強化的循環：



七、 資訊安全與客戶隱私之管理架構

保護機密資訊與維護客戶隱私，始終是本公司長年與客戶維繫合作關係並建立信任基礎的關鍵因素之一。

本公司深知，客戶在業務往來過程中所提供的資訊，皆屬於極具價值之資產，因此我們將「確保客戶資訊安全」視為最核心、最重要之資訊安全管理目標之一；唯有持續投入資源，並將資訊安全與隱私保護列為營運核心價值，方能與客戶建立長久穩固之互信合作關係。



八、 資訊安全之風險

本公司依循「上市上櫃公司資通安全管控指引」及「ISO 27001:2022」國際標準，已建置一套完整且符合國際規範之資訊安全管理制度，並依循該制度規劃與導入符合公司營運需求之資訊系統與資訊安全設備。此制度不僅涵蓋技術防護措施，亦包括組織管理制度、作業流程規範及人員之安全意識教育，以形成全面性的資訊安全防護網。

為確保制度之有效性與持續改善，本公司每年均定期檢視並更新相關規章、控制措施與作業程序，同時執行資訊安全風險評估，以即時掌握潛在威脅與弱點，並依據檢視結果進行調整與優化，確保制度能持續符合實際營運環境及法規要求。

然而，本公司亦深知資訊安全風險具有高度不確定性，且隨著科技快速演進與資安威脅持續變化，任何制度皆有可能面臨挑戰。基於此，本公司將持續透過 PDCA 持續改善機制、定期內外部稽核、資訊安全事件演練及專業資安顧問之協助，不斷強化資安治理能力，並採取多層次防禦策略，以降低風險對公司營運及客戶權益所可能造成的影響。

本公司相信，唯有以嚴謹的管理制度與持續改善的態度，方能有效確保資訊資產之機密性、完整性與可用性，進而維護公司聲譽並鞏固客戶及合作夥伴的信任。

九、 辦理資通安全宣導執行情形

本公司除每季定期發布資訊安全公告外，亦將視情況針對特定議題進行不定期之宣導與溝通，以持續提升全體同仁對資訊安全議題的認知與重視。透過定期與即時並行的方式，確保資訊安全政策能有效落實於日常作業中，並提升組織整體的資安防護能力。

本公司已正式制定「風險管理政策與程序」，以系統化方式進行資訊安全相關風險之識別、評估、監控與應變，並將風險管理成效納入組織治理架構，確保資訊安全作為公司治理之重要一環。依據該程序規範，本公司已於 2025 年度將資訊安全風險狀況及相關執行情形提報董事會，以供高層管理階層及董事成員進行審視與決策參考。

截至 2025 年 09 月 30 日止，本公司並未發生重大資通安全事件，亦無因資安事件而造成可辨識之重大營運或財務損失。對於外部主管機關所要求揭露之資訊，本公司均依規定進行檢視與確認。截至目前，對於可能影響或潛在風險所帶來之損失、影響及因應措施，若有無法合理估計者，亦已據實說明其無法合理估計之事實；惟經評估，目前並無相關事件發生，故本公司揭露內容為：無。

本公司將持續依循 PDCA 管理循環與風險控管機制，強化資安事件預防、應變與通報程序，並透過定期稽核、教育宣導與持續改善措施，妥善確保公司資產及客戶資訊安全，進一步提升營運永續能力及企業信譽。