正達國際光電股份有限公司
南科分公司
資訊安全政策

核 准	審 查	制 定

修訂履歷

版本	日期	說明	備註
V1.0	2025.10.1	首次發行	

目錄

1. 目的

鑑於資訊安全乃維繫各項資訊服務安全運作之基礎，為確保本公司具備共識落實資訊安全的使命，特訂定本資訊安全政策（以下簡稱本政策），做為本公司資訊安全管理系統的最高指導原則，以確保本公司管轄資訊資產之機密性、完 整性、可用性及符合相關法規之要求，進而保障全公司人員及客戶之權益。

2. 適用範圍

本公司員工、接觸本公司業務資料之外機關人員、委外服務提供廠商人員及訪客。

3. 名詞解釋

3.1 機密性（Confidentiality）：確保只有經授權的人員才能存取相關資訊資產。
3.2 完整性（ Integrity ）：維持資訊資產之正確與完整。
3.3 可用性（Availability）：確保經授權的人員在需要時，均能在可接受的時間內取得相關資訊資產。
3.4 核心系統：本公司 ISO/IEC 27001 驗資訊安全管理制度之驗証範圍或實施範圍內之重要系統（如：作業系統、網站應用程式、資料庫、與其閘道端網路保護軟硬體）。
3.5 資訊安全：係避免因人為疏失、蓄意或自然災害等風險，運用系統化之 控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保 本公司資訊資產受到妥善保護。
3.6 資訊資產：凡本公司作業流程中使用之資訊資產，如內部人員、外部人員、 紙本文件、電子文件、網路服務、電腦應軟體、應用系統、電腦硬體、 網路設備、環控系統、建築保護設施與便利設施等皆屬之。

4. 組織與權責

為確保資訊安全管理系統能有效運作，應明定資訊安全組織及權責，以推動及維持各類管理、執行與查核等工作之進行。

5. 要求事項

5.1 資訊安全目標
　5.1.1 本公司依照適用之法律法規要求、提供客戶專業之客戶服務。
　5.1.2 為確保客戶服務品質，確保公司持續營運、保障客戶資訊安全之權益，本公司資訊安全目標為確保核心系統管理業務（意即 ISO/IEC 27001 驗證範圍內之資訊系統與相關管理活動）之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability），依「風險管理程序」與「資訊安全目標管理程序與績效管理程序」定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

5.2 審查與評估

5.2.1 本政策應至少每年評估審查一次，考量法令法規、科技變化、利害相關團體之需求與期望、業務活動、內部管理與資源等最新現況，確保資訊安全實務作業之有效性。

5.2.2 本政策應依據審查結果進行修訂，修正時亦同。

5.2.3 本政策訂定或修訂後應以適當方式（例：E-Mail 或網站公告/紙本印出/稽核時提供/客戶要求時提供）告知利害相關團體，如：所屬員工、供應商、客戶、外部稽核人員等。

6. 資訊安全管理系統

依據 ISO/IEC 27001 指導規範之『規劃—執行—檢查—行動』模式，發展、維護及持續改善文件化的資訊安全管理系統，內容說明如後：

6.1 安全政策

訂定資通安全政策做為資訊安全管理系統的指導方針，經由管理階層核准、頒行，並透過適當管道，宣導給全體同仁，且於重大改變時或定期審查，以確保其適當性 與有效性。

6.2 全景分析

透過風險評鑑會議或其它型式會議，考量內外部議題與利害相關者要求進行全景分析。

6.3 資訊安全組織

成立資訊安全組職並賦予相對權責，以建置與維運此系統。

6.4 人力資源安全

6.4.1 將資通安全職責載入人員之工作職掌或僱用合約中，且人員須簽署該份文件。

6.4.2 管理階層須要求人員遵循既定的安全規範。

6.4.3 政策與程序須透過適當的教育訓練，告知相關人員並定期更新。

6.4.4 所有人員於離開工作崗位時，須按照既定的程序辦理相關資產退回與存取權限的變更或取消。

6.4.5 違反資安規範時，須施以適當的懲戒，以確保安控規範之實施成效。

6.5 資產管理

6.5.1 鑑別所有資產，將重要的資產作成清冊並維護之。

6.5.2 所有資訊資產都要指派專人管理。

6.5.3 根據資訊本身的價值、法律上的要求、敏感性或重要性等因素，區分其等級並做適當的標示，以妥當保護資訊資產。

6.6 存取控制

6.6.1 須有存取控制機制文件，以便遵循。

6.6.2 核心系統或關鍵業務流程應有使用者註冊、變更與刪除流程並定期審查權限。

6.6.3 使用者使用資訊處理設施，須設定使用密碼。

6.6.4 訂定辦公桌與螢幕淨空措施。

6.6.5 訂定網路服務機制，以維護網路安全。

6.6.6 訂定遠端連線時限與系統連線時限，以保護系統安全。

6.6.7 訂定應用系統之存取控制與隔離機制，以保護其相關的資訊。

6.7 密碼學

6.7.1 若使用金鑰加密資訊（如：購買之 SSL 數位憑證/終端機連線金鑰/憑證），應妥善保管金

鑰，且熟悉如何更新（或下載）金鑰與汰換。

6.7.2 非公開資料資訊（如：個資或營業秘密）的傳輸或保存，應視實際需求予以加密或其它安全保護方式。

6.8 實體及環境安全

6.8.1 規範實體安全界限、進出管制方式、保護辦公處所及設備、載明在安全區域中工作的規範。

6.8.2 設備妥為安置與保護、提供適當服務之公共設施（包括電力、空調、消防）、傳輸線需考慮其佈置安全性，及有適當的方法保護在公司內、外使用的設備。

6.9 作業（運作）安全

6.9.1 以實際系統運作狀況規劃資訊處理設施的需求，且採購時要確實執行驗收工作；設施運作時若需變更，須依據變更管理程序執行系統變更。

6.9.2 建立防範惡意程式碼之機制。

6.9.3 定期備份核心系統資料，以維持服務之完整性與可用性。

6.9.4 隨時監督系統使用狀況，並記錄之，同時妥善保存核心系統軌跡紀錄(Logs)，以防止遭受竄改或破壞。

6.10 通訊安全

6.10.1 須有網路安全控制機制（如：防火牆）以維護網路安全。

6.10.2 業務應用系統、電子商務、電子郵件與即時傳訊軟體（Instant Messenger）等，均須有適切的保護措施。

6.10.3 資訊傳遞應視資訊機密等級，予以安全地傳送。

6.11 供應商關係

6.11.1 資通訊委外服務應於合約或第三方協議中考慮資訊安全要求。

6.11.2 應定期或不定期監督供應商服務過程是否符合本公司資安要求。

6.11.3 應確保第三方之複委託機構亦應遵守本公司資安要求。

6.11.4 合約變更、調整應以不影響本公司資訊安全為最高原則。

6.12 資訊安全事故管理

6.12.1 人員有回報資安事件、弱點與軟硬體失能的責任，並從中學習以改善資訊安全環境。

6.12.2 訂定資訊安全事件/事故管理規範。

6.12.3 確實記錄與蒐集相關資安紀錄。

6.12.4 定期彙總分析資訊安全事件/事故，以採取適切的管控措施。

6.13 營運持續管理

6.13.1 明訂營運持續運作的管理流程。

6.13.2 執行營運持續運作的計畫。

6.13.3 審查營運持續運作計畫的結果，以維持其適合性。

6.14 遵循性管理

6.14.1 鑑別適用的法令及規章，以確保法規與密碼學要求的符合性。

6.14.2 訂定使用智慧財產之相關要求。

6.14.3 保障個人資訊與隱私權。

6.14.4 妥善保守公司重要之資訊紀錄。

6.14.5 定期審查安全政策與技術之符合性。

6.14.6 依「管理審查程序」週期性的對資訊安全管理系統進行審查及確認，資訊安全的控制目標、控制措施、政策、過程及程序的作法。透過稽核制度防止舞弊事件。

7. 參考文件

7.1 本公司 ISMS 一階至三階文件與相關表單。