友達資訊安全政策與治理方針

友達資訊安全政策

「保護公司智慧財產，全面提昇資安意識，共創贏(盈)的契機」為本公司資訊安全之核心理念。本公司高度重視資訊安全，視其為企業永續發展的重要基石，以保護客戶、公司及利害關係人之重要資訊資產為目標，持續強化整體資安治理與防護能力。

友達資訊安全承諾

本公司承諾持續精進資訊安全治理，並致力於：

- 持續完善資訊安全管理系統，提升資訊資產整體防護能力
- 確保資訊資產之機密性、完整性與可用性，涵蓋客戶資料、個人資料及公司自有資料
- 持續監控並有效回應資訊安全威脅與事故，降低對營運及利害關係人之衝擊
- 落實全體員工之資訊安全責任與當責文化，強化資安意識與日常遵循
- 強化供應鏈與合作夥伴之資訊安全要求，共同維護資訊生態系統之安全

資安治理架構

本公司由董事會層級之永續暨風險管理委員會統籌監督資訊安全風險，並透過專責治理機制將資安納入企業整體風險管理架構中。同時設立資訊安全委員會負責審議資安政策與策略，並由資訊安全長領導專責單位及跨部門團隊推動各項資安工作，確保資安治理由上而下有效落實。

標準遵循與認證

本公司參考國際標準（包含但不限於ISO/IEC 27001）建置資訊安全管理系統（Information Security Management System, ISMS），透過制度化、文件化及系統化之管理機制，持續強化資訊安全管理能力與營運韌性，規劃資安策略與行動方案，確保資安管理與公司整體營運發展方向一致，並取得相關認證（包含但不限於ISO/IEC 27001）。

法規遵循與隱私保護

本公司遵循相關資訊安全與個人資料保護法規（包含但不限於GDPR），並制訂隱私權政策，說明個人資料蒐集、處理、利用及當事人權利保障機制。

風險管理與防護機制

本公司透過系統化風險評鑑機制，定期識別與分析資安風險，並將其納入企業整體風險管理流程中，以確保重要資產受到適切保護。同時透過多層次防護策略，包含系統防護、弱點管理、事件偵測與回應機制等，持續強化資安防禦能力與應變效率。

存取控制與資料保護

為確保資料安全，本公司依最小權限原則（Least Privilege）管理使用者存取權限，並導入多項管理與技術控制措施（包含但不限於多因子驗證、傳輸與儲存加密機制），確保資訊於全生命週期皆受到妥善保護。

資安事件管理與通報機制

本公司建立資安事件應變程序，涵蓋事件偵測、通報、分析、遏止與復原等流程，以降低事件衝擊。於發生重大資安事件時，將依相關法規及契約要求，於適當時限內通知相關利害關係人及主管機關。

營運韌性與持續營運

本公司建置營運持續計畫（BCP）及災難復原機制（DR），透過備援設計、資料備份、復原機制與定期演練，確保關鍵系統及業務於災害發生時可於可接受時間內恢復運作。

資安文化與員工責任

本公司致力推動全員資安文化，透過教育訓練、宣導活動與制度規範，強化員工對資訊安全之認知與遵循，並落實資安共責與當責之管理理念。

供應鏈與生態系安全

本公司將資安管理延伸至供應鏈與合作夥伴，要求供應商及合作夥伴遵循資訊安全相關規範，並透過評估、契約條款及定期管理機制，共同提升整體資安防護水準，建立安全且可信賴的產業生態系。

系統開發與技術安全

本公司於系統開發生命週期（SDLC）中導入資安要求，包括安全設計、程式碼檢視、弱點掃描及滲透測試，並落實系統變更與漏洞修補管理，以降低系統風險。

績效、持續改善與稽核

本公司訂定資安績效指標（如弱點修補率、事件回應時效、訓練完成率等），定期監控與檢討，以確保資安管理之落實與持續改善。本公司透過內外部稽核機制，定期檢視資訊安全管理制度之有效性，並由管理階層進行審查，持續精進資安治理與控制措施。

持續合作與產業參與

本公司積極參與產業資安合作與人才培育，透過跨組織交流與專業合作，共同強化整體社會之資安韌性。

數位長 謝忠賢

Version 1, July 2026