迅得機械資通安全管理政策
114 年 11 月 11 日董事會報告

附件 D

一、 資通安全政策

1. 目的

・資通安全是各項資通服務運作之基礎，為維護迅得機械股份有限公司（以下簡稱本公司）之全體人員、資通系統、存儲資料、設備及網路的安全運作，特訂定資通安全政策（以下簡稱本文件）作為最高指導原則。

2. 範圍

・凡公司全體同仁、客戶、委外或合作廠商、供應商、第三方人員以及所有相關資通資產之安全管理，應依資通安全政策處理。

3. 內容：

・本公司以至誠服務之態度提供良好品質，以達客戶滿意。積極、主動地、創新及改良、秉持品質為優先，配合市場之成長及滿足顧客要求，為保護利害關係人之資通安全與權益，訂定資通安全政策。

・為確保資通系統能更有效運作，明定資通安全組織及權責，以推動及維持各類管理、執行與查核等工作。

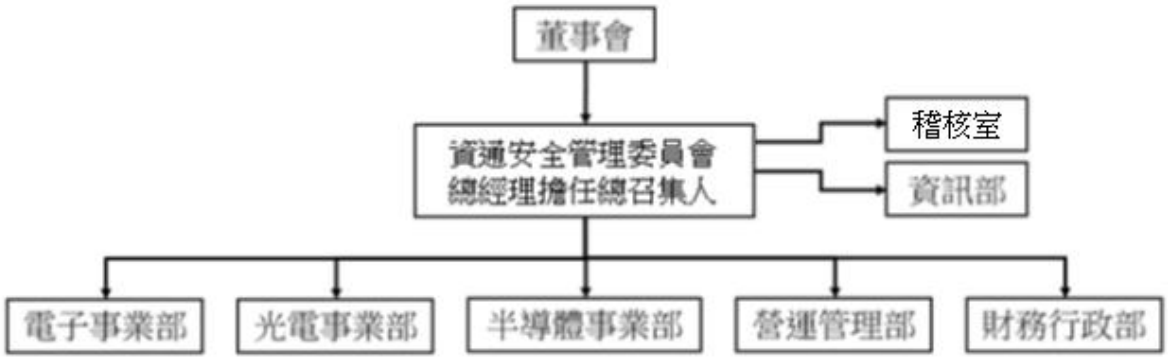
・資通安全管理系統依據 PDCA 模式實施，以不間斷、循序漸進的精神，確保資通服務運作之有效性及持續性。

・為反映相關法令法規、科技變化、客戶期望、業務活動、內部環境與資源等最新現況，資通安全管理委員會定期檢討資通安全政策，並每年至少一次向董事會報告當年度資通安全管理執行情形。

二、資通安全管理架構

1. 本公司成立資通安全管理委員會，掌管營運所需之資通科技相關事項，由總經理擔任主席(召集人)，資訊單位最高主管擔任資訊安全主管，統合各事業單位、資訊、稽核等單位之最高主管組成，不定期召開相關會議，以進行資安事務之決策、管理與推動，落實企業經營者的責任，保障股東的合法權益且兼顧其他利害關係人的利益。

2. 資通安全管理架構：



3. 以「風險管理」之角度推行控管，定期自我評估資通管理能力，透過

資通安全稽核持續優化，形成改善與強化之管理循環，並確保各項業務運作順利。

4. 建立威脅情資分析與預警機制，透過集團、子公司與外部單位的情報分享，提供資安事件資料、報表及其他資訊，協助公司提升資通安全管理系統。
5. 落實通報程序與應變措施，提昇內部人員面對突發狀況之應對與協調能力，將資通安全事件帶來的損害極小化，以此提升公司韌性。

三、資通安全具體管理方案

1. 各項服務品質嚴格要求，通過 ISO 9001 管理標準。資訊科技、安全技術、資訊安全管理系統要求，透過 ISO 27001 建立起資訊安全管理系統的機密性、完整性與可用性，以確保資訊資產的安全、降低資安風險。
2. 訂定資通管理政策，並依循公司資通安全相關內部控制制度，結合 PDCA 方法力求逐步精進，以保護人員、資料、資通系統、設備及網路之安全等機密性、完整性、可用性、遵循性。
3. 高階主管積極參與資通管理活動，提供支持及承諾。
4. 定期召開資通管理會議，反應政令法規、外內部風險、科技技術及業務需求等最新發展，以達到利害關係人期待。
5. 以風險控管出發，評估並降低風險，以確保資通資產之機密性、完整性、可用性、合規性。
6. 引進新式技術，佈建即時監控設備與防護系統，積極深化機密資通保護機制，提昇整體資通環境之安全性，降低各項風險發生率，以保障客戶、合作夥伴、利害關係人之利益。
7. 本公司之存取權限與存取控制的主題特定政策如下：
   - 限制對資訊及資訊處理設施之存取；
   - 確保授權使用者得以存取，並避免系統及服務的未授權存取；
   - 令使用者對保全其鑑別資訊負責；
   - 防止系統及應用遭未經授權存取。
8. 持續進行各項營運演練活動，以確保公司服務面對外部威脅時，可以快速因應，展現公司韌性。
9. 依照個人資料保護法、資通安全管理法等相關規定，審慎處理、保護個人資訊及其相關系統安全。
10. 落實資通安全稽核，確保本公司各項業務恪遵相關政策，使資通管理制度持續正常運作。

114 年度資通安全執行情形

一、本公司為強化公司資通安全管理，確保資料、系統、設備及網路等軟硬體資通安全，營造健康的資通環境，部署創新的資通安全防護技術，推動資通安全管理作業，公司於 110 年 10 月建置資通安全管理政策及架構、成立資通安全委員會及制定相關資通安全規範，確認資通安全管理運作之有效性，並每年一次向董事會報告執行情形。

二、114 年度辦理 1 次異地備援演練：

1. 模擬情境：災害發生時，迅速將系統環境資料移轉至另一系統主機上。
2. 回復時間：2025/04/03~2025/04/06 SPA(Production)正式區主機資料
3. 還原環境：SQA(Test)測試區主機
4. 請相關部門確認比對測試區環境資料是否正確-20250408

三、114 年度辦理資通安全設備更新報告：

年度	公司	項目	完成度
2025	集團	社交工程演練	進行中
	SAA	資安弱點偵測	進行中
	SAA	新生廠資訊系統建置	進行中

四、更新後成效：

1、資安弱點偵測

因應台積電供應鏈資安要求，導入外部資安弱點偵測系統，提升資訊安全。(共花費 NTD$59,850)

2 、社交工程演練

3/6（四）社交工程第二次課程，上課人員 SAA,SAC,SAE,SAH。(共花費 NTD$150,000)

五、115 年度計劃辦理資通安全設備更新項目：

年度	公司	項目	完成度
2026	集團	集團點對點 VPN 設備汰換	進行中
		端點控管系統	未開始
	SAA	資安弱點偵測	進行中
		社交工程演練	

六、預計更新後成效

1、VPN 負載平衡器因無法繼續簽訂維護合約，為確保集團內各廠域之間交換數據等流量更加穩定，故預計汰換。

2、建置端點控管系統，增加使用者電腦設備之安全防護。

3、進行資安弱點偵測，加強資訊設備弱點防護。
4、進行社交工程演練，加強使用者網路資訊安全意識。

七、114 年度共執行 12 次資通安全宣導：
1、提防 Quishing！別讓 QR Code 成為資安破口！ - 20250402
2、釣魚信 + OneDrive 對台日展開高隱匿間諜行動 - 20250620
3、帳密資料外洩與 DDoS 攻擊的規模雙雙創下新高 - 20250708
4、資安廠商發現聯想（Lenovo）電腦中一個預載檔案被可寫入資料，可能破壞 Windows 的 AppLocker 提供的安全防護 - 20250716
5、Cisco 針對 NX-OS 零時差漏洞 CVE-2024-20399 提出警告 - 20250801
6、三項議題：第一議題-公司內帳戶被惡意人士盜用，第二議題-line 近期盜用成長為 80%，第三議題-line 分享螢幕導致帳戶被盜領 - 20250811
7、Fortinet SSL VPN 設備遭遇大規模暴力破解攻擊 - 20250814
8、GitHub Actions 成內鬼溫床，寫入權限竟等同全權存取！；AWS 阻止 APT29 水坑攻擊，避免微軟帳號遭竊用；已棄用的搜狗輸入法更新伺服器遭入侵，駭客用於對多國網路間諜活動 - 20250902
9、歹徒冒名奈米醫材旗下投資公司發動商業郵件詐騙，MostereRAT 瞄準 Windows，利用 AnyDesk 和 TightVNC 實現完全訪問，GPUGate 惡意軟體利用 Google 廣告和虛假 GitHub 攻擊 IT 公司 - 20250911
10、TSMC 供應鏈 - 致茂先進 遭駭客勒索、解密「長線佈局」與跨領域攻擊：CrowdStrike 深入解析 2025 駭客戰術演進 - 20250918
11、中國 APT 組織 Phantom Taurus 連續三年攻擊微軟 Exchange 伺服器-20251001
12、Discord 稱駭客竊取了 1.5TB 資料，70,000 張身分證照片 , Stealit 惡意軟體利用 Node.js 隱藏在虛假遊戲和 VPN 安裝程式中 - 20251013

八、資訊安全教育訓練
114 年度資訊安全教育訓練上課名單

部門	姓名	職等	上課日期	備註
資訊部	全員	—	3/6	社交工程演練
資安組	呂昆晏	資深工程師	4/16	人工智慧及資安風險
資安組	呂昆晏	資深工程師	4/18	資訊安全管理系統

訓練成效:
1、參加社交工程演練，提升資訊安全意識。
2、參加人工智慧及資安風險、資訊安全管理系統等課程，了解資安風險及管理方法。

九、ISO/IEC 27001:2022 稽核
為維護本公司之全體人員、資通系統、存儲資料、設備及網路的安全運作，特

導入 ISO/IEC 27001:2022 版作為最高指導原則，每年定期稽核。

資訊安全委員會	負責人員與聯繫方式（分機或手機）
召集人	黃發保 總經理 #508
管理代表	林肇德 副總經理 #128
資訊組	洪又文 #355，曾翊倫 #39，蔡政勳 #357
資安組	李信忠 #370，呂昆晏 #356