

迅得機械資通安全管理政策
113 年 11 月 12 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，並參酌國際資通安全標準制定相關規範。
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. 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。
8. 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。
9. 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。

113 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、113 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：2024/06/08~2024/06/11 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-20240617

三、113 年度辦理資通安全設備更新報告：

年度	公司	項目	完成度
2024	集團	資產管理系統	進行中
		社交工程演練	進行中
	SAA	資安弱點偵測	進行中
	SAC	VMWare Server 汰換	完成

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、SAC VMWare Server 汰換

原 VMWare 硬體年限已到，且無法再擴充更新，故更換系統，提升系統穩定性及運行效率。(共花費人民幣 1,136,900)

3、社交工程演練

8/20 (二) 社交工程第一次課程，上課人員 SAA, SAC, SAE, SAH。(共花費 NTD\$150,000)

五、114 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
2025	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、113 年度共執行 5 次資通安全宣導：

- 1、資安通報：近期駭客組織開始活絡，勒索軟體駭客組織 Red CryptoApp 聲稱入侵超過 10 個企業組織，詳細內容請詳閱內文說明-20240503
- 2、資安通報：駭客組織利用系統漏洞成功入侵教育部導致資料外洩，詳細內容請參閱內文詳述-20240515
- 3、資安通報：Phoenix UEFI 韌體存在高風險漏洞-20240701
- 4、資安通報：VMWare ESXi 遭勒索軟體的駭客組織濫用-20240731
- 5、資安通報：中國駭客 TIDrone 鎖定臺灣衛星及軍事工業、3 家上市公司遭遇 DDoS 攻擊 -20240913

八、資訊安全教育訓練

113 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
資安組	李信忠	經理	5/4~5/18	CISSP, 取得上課證明
資訊組	洪又文	副理	5/4~5/18	CISSP, 取得上課證明
資安組	李信忠	經理	6/28	台積電供應商資安大會
資安組	呂昆晏	資深工程師	6/28	台積電供應商資安大會

訓練成效：

- 1、參加 CISSP 資安課程，符合並滿足資安稽核需求，並提升資訊安全意識。
- 2、參加台積電供應商資安大會，了解客戶及半導體業資安要求。

九、導入 ISO/IEC 27001:2022 版

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。

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 #391，蔡政勳 #357
資安組	李信忠 #370，呂昆晏 #356