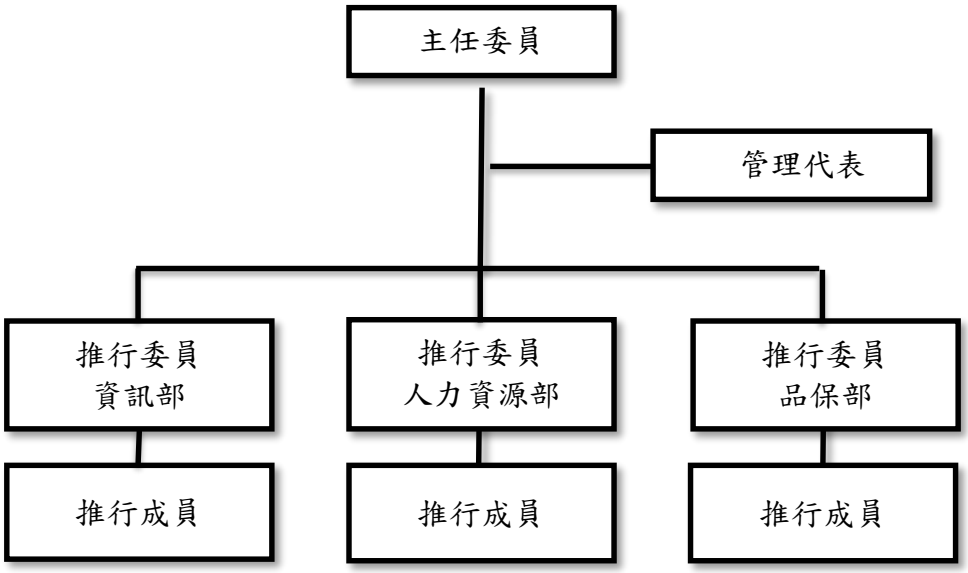
振曜科技股份有限公司
資通安全管理

(一)資通安全風險管理架構

1.振曜科技設置資訊安全主管及資訊安全管理委員會，委員會成員共計 7 人，組織圖如下：



2.振曜科技已於 2024 年 12 月 31 日取得新版 ISO/IEC 27001:2022 國際認證，驗證效期至 2027 年 12 月 30 日。

3.振曜科技 2025 年召開 ISO27001 相關之資通安全管理審查會議共 2 次。

(二)資通安全政策、具體管理方案及投入資通安全管理之資源等

振曜集團已訂定資通安全檢查之控制作業辦法，由資訊單位負責管控及維護資訊安全，透過定期檢視和評估其安全規章及程序，確保其適當性和有效性。

1.作業程序

(1)資料經由電子郵件傳送或接收時，系統應設置防火牆及防毒軟體，以防止駭客或電腦病毒之侵害。

(2)員工應避免透過公司網路收發或下載與業務無關之郵件或軟體，以避免佔用公司之網路資源及增加電腦病毒感染的機會。

(3)公司員工非經權責主管授權，禁止將公司相關資訊經由電子郵件對外傳送。

(4)公司有關資訊硬體之報廢、送修及移轉使用均應會辦資訊處理部門，可重複使用之資料儲存媒體與設備，不再繼續使用時，應將儲存之內容銷除後再進行報廢或銷毀。含有儲存媒體之設備(如硬碟)，在處理(報廢、送修、移作其他用途)前應由資訊處理部門詳加檢查，以確保任何機密敏感資料已經移除。

2.控制重點

(1)公司郵件伺服器是否有裝設防火牆及防毒軟體，以隔絕外來侵害。

(2)公司電腦是否安裝防毒軟體及更新病毒碼並定期進行病毒掃描。

(3)資訊設備報廢、送修及移轉使用，是否會辦資料處理部門，並確實檢查儲存資料是否已移除。

現今科技日新月異，資訊系統網路應用層面日漸廣泛，除了帶來更多效益，也

潛藏了一定的網路威脅，振曜集團針對明顯及潛藏的威脅亦作了一些防護及規劃。

1.主機及個人電腦設備防範：已部署EDR系統，安裝具有端點保護的軟體進行防護，並具有黑白名單、沙箱機制防護。

2.已設置備份軟體具有資料防護功能：備份的作業系統影像或應用程式可能存在漏洞，如果惡意軟體仍存在於網路，可能會導致持續重新感染。修補裝置並套用最新的防惡意軟體定義，可以最新的修補程式還原作業系統影像，降低再次感染的機會。

3.已架設防火牆Firewall來保護、管控整個企業內網，並設定管制條例進行適當的安全及權限設定；VPN網路服務亦可納入管理，藉此保護使用者透過公用網路安全地瀏覽和存取個人資料。

4.持續補強及導入資訊安全產品功能，期望強化公司整體資訊系統之安全。

5.振曜科技已於民國113年12月31日取得新版ISO/IEC 27001:2022國際認證，藉由國際認證且通用的「資訊安全管理」標準流程，幫助公司持續改善組織資訊系統、防範內部資訊安全可能出現的漏洞。導入ISO/IEC 27001:2022新版標準，不僅檢討了原有的2013版程序並加以調整控制項目，甚至涵蓋廣度將增加資訊安全、網路安全與隱私的保護，以更符合現代的資安管理需求。2025年成功通過複驗稽核。

(三)最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施

1.事件說明

振曜集團於2025年03月31日上午確認公司網站遭駭客竄改，同時亦發現部分主機上的檔案被加密。經調查係駭客使用破解之帳密登入官網後台進行竄改，並將勒索軟體下載至主機系統執行加密，已委託外部資安公司協助偵測病毒並恢復日常作業。

2.產生之影響

公司網站已聯絡代管服務廠商重設帳密並回復正確資料。另資料被加密之主機以備份資料重建，此外，本公司生產基地以大陸地區為主，並未遭受網路駭客攻擊，對公司營運尚無重大影響。

3.因應措施

發現遭駭客攻擊後，振曜集團立即切斷對外網路，並第一時間聯絡外部資安公司進廠調查。除清理並恢復受影響主機外，同時取得惡意程式樣本，後續委託資安公司進行樣本分析以確認攻擊全貌，另進行全廠區資安檢測，以確定是否有殘留之威脅，並於2025年更新EDR系統。