微端科技股份有限公司
資訊安全管理報告

日期:2024/3/1

前言：

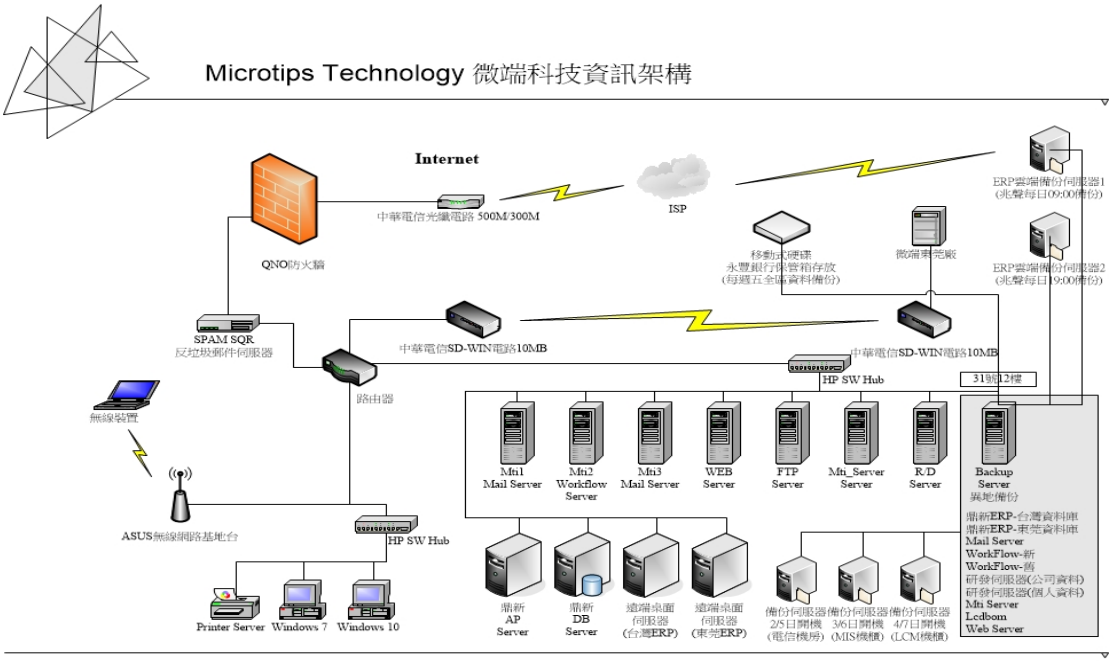
為保護微端科技股份有限公司（以下簡稱本公司）產品與服務之資訊，避免有未經授權之存取、修改、使用及揭露，以及天然災害所引起之損失，並適時提供完整與可用之資訊，本公司致力於資訊安全管理，以確保本公司重要資訊財產之機密性、完整性及可用性，並符合相關法令法規之要求，進而獲得客戶信賴、達到對股東的承諾，保證公司重要業務持續運作。

近年來資訊社會日新月異、資訊的發展網路的延伸，資安風險也日漸升高，甚而影響企業的運作或財務、業務的損失。公司之於資安風險，業建置資訊安全風險營運管理機制因應，如「內部控制-資訊循環」、「內部重大資訊處理及內線交易管理」、「個人資料保護之管理」及「電腦作業管理辦法」等相關資訊安全風險管理機制營運，提供所有員工落實遵循，以保障所有利害關係人之權益、公司經營之成果。

資訊安全管理機制：

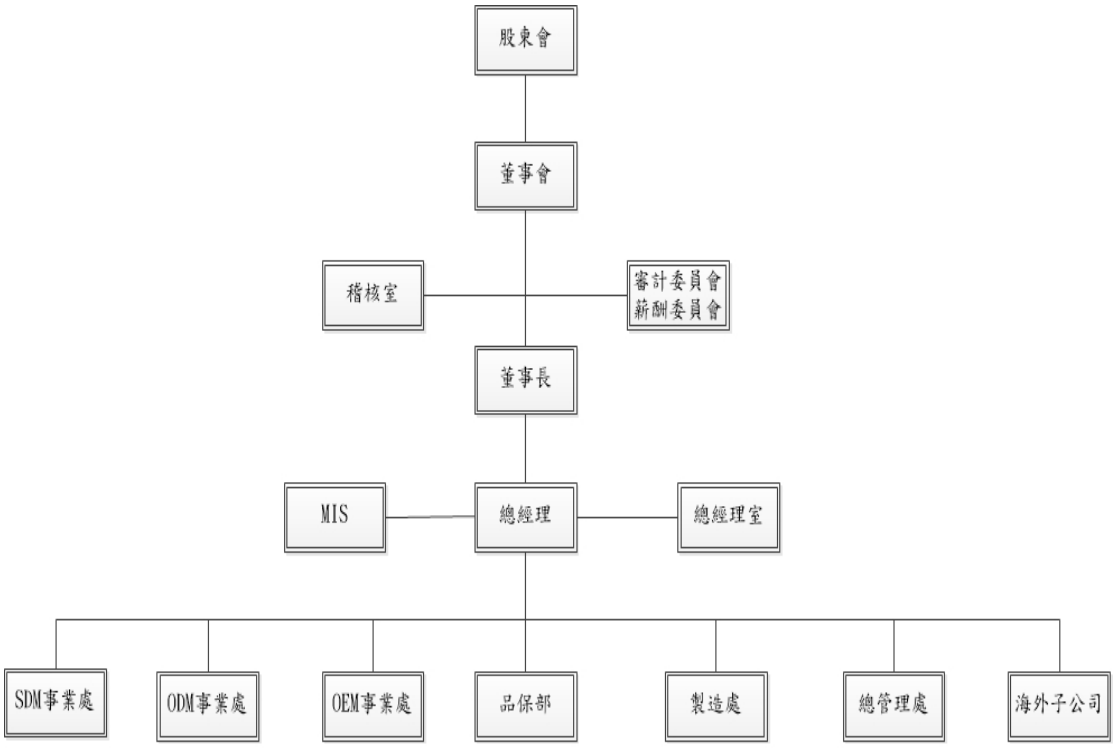
有鑑於新型態的資安威脅，如勒索軟體、社交網路攻擊、電子郵件詐騙…等威脅日益增多，透過調整資安政策，提升內外連線防護以及落實備份，並定期安排弱點掃描與滲透測試，全面提升資安防護能力。

資訊安全策略	
資安治理	優化管理機制 降低風險與防範，與時俱進優化管理機制、強化教育訓練、資訊安全與管理落實執行。
內外連線	升級次世代防火牆、換裝中華電信SD-WIN專線連接東莞廠，可有效提升威脅防護、降低公司營運成本。
備份系統	提昇硬體備份環境，並使用外部雲端應用分散風險。

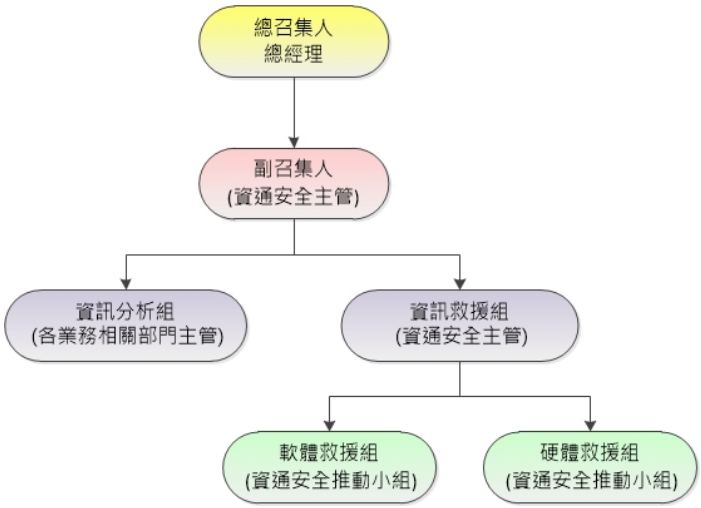


資安管理單位：

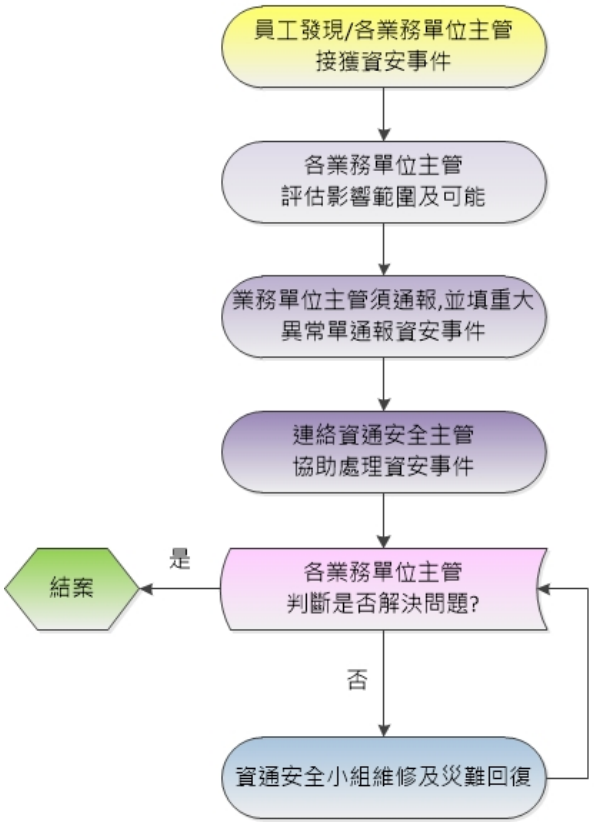
1. 資安管理單位為資訊安全室(MIS)，負責審視公司資安管理政策、規劃、監督、資安運作情形，隨時監控資安管理運作情況。遇重大資安風險事件，及時向總經理報告，定期評估資訊安全風險並向董事會報告。
2. 公司有使用資訊系統之人員，每年接受內部資訊安全教育訓練課程，每人每年至少三小時,另負責資訊安全之主管及人員,每年接受外部資訊安全專業課程。
3. 為預防勒索軟體,必須先對勒索軟體的攻擊途徑有所瞭解。本公司加入 TWCERT 台灣電腦網路危機處理暨協調中心會員，不定時接收 TW-ISAC 通知信-情資發送，做為事前預防、事中處理及事後回復之參考依據，將資安的攻擊面縮減到最少。
4. 各組織及流程圖：



跨部門資通安全小組組織圖



資通安全事件處理流程

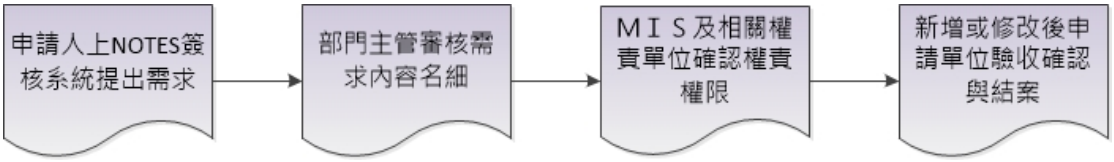


資訊服務流程管理：

為確保公司所面臨之風險得以控管，本公司對資安風險進行評估，將資訊安全機制分為實體安全、軟體安全、網路安全及作業安全四個面向，透過內部ＮＯＴＥＳ系統運作流程、人員授權及職責分離、文件及資訊流向管理等控制措施，並定期異常查核，以利及時反應處理。

本公司各單位人員需求資訊應用軟硬體、系統、郵件、網路等資源權限之申

請及異動，以電子流程申請程序，經有關權責主管審核、確認援權後辦理。



資訊安全管理方案：

本公司檢視資安風險經風險辨識與風險評估，確認該資安風險對企業經營不利之影響程度，採取相應管理措施，並針對資訊架構檢視、網路活動檢視、網路設備、伺服器及終端機等設備檢測、安全設定檢視等重點，隨時檢視及評估有無漏洞或設備老舊問題，也因應資訊安全所面臨的挑戰，如 ARP 進階持續性攻擊、DDoS 攻擊、勒索軟體、社交工程攻擊、竊取資訊等資案議題。

規劃資訊安全管理方案如下：

1. 網路防火牆設置：阻擋外部的惡意攻擊，防止駭客入侵。
2. 防毒軟體設置:防護內部電腦,防止不明郵件或釣魚網站植入病毒或木馬程式。
3. 系統程式資料存取控制：嚴格控管及申請程序，保護資料不外洩。
4. 電子郵件管理控制：做好郵件管控及防護機制降低外部郵件的攻擊。
5. 資訊系統災難恢復計畫：每年一次災難復原計畫的演練。

資訊安全管理投入資源：

為了強化資通管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之業務持續運作之資訊環境，並符合相關政府法規與內外部利害相關者之要求，使其避免遭受內、外部的蓄意或意外之任何威脅，達到資訊安全，本公司設有資通安全管理辦理辦法。本公司資訊安全管理系統，適用範圍設定為資訊機房維運、業務運作系統及網站系統維護之安全管理，已充份掌握資訊運作及管理過程並滿足各項安全要求與規範，

具體管理方案及投入資通安全管理之資源如下:

1. 確實遵守「個人資料保護法」、「著作權法」、「智慧財產管理制度」等資訊安全相關法令。
2. 保護本公司業務活動資訊，避免未經授權的存取、修改，確保其正確完整。
3. 尊重智慧財產權，保護顧客及公司資訊，員工需填寫智慧財產保密表格確保保密責任。
4. 確保所有資訊安全意外事故或可疑之安全弱點，都應依循適當之通報機制向上反映，並予以適當調查及處理。
5. 使用具合法版權軟體、避免上網下載來路不明軟體，及瀏覽不明網站。
6. 若有來源不明之電子郵件，不隨意點擊內容連結及下載附件檔案。
7. 不定時更新作業系統及防護軟體病毒定義檔。
8. 訪客個人手機及個人電腦限制只可使公司訪客網際網路，未經允許嚴禁連接公司內部區域網路

資安事件與保險：

本公司資安治理、管理機制之運行，於全體員工依據規定落實執行，並未發生嚴重資安事件，整體資訊安全風險管理得宜，可達預期目標。公司在實體資產已有保險、且主要檔案資料採取異地備份，暨各系統災害復原計劃，如未來法令規範、資安管理需求需投保資安險，屆時公司將評估了解其相關規定及配套措施再決定。

資安風險管理檢視與改善：

資訊管理單位，每年進行一次全公司資通安全檢查控制，檢視與公司資安策略、風險管理機制，落實執行或需求改善之處。並與時俱進，因應法令更新或營運需求，修訂資訊安全管理方案機制、編制資訊安全風險管理需求資源或配置，提供經營階層參考或改善依據。

112 年度執行情形如下：

1. ERP 進銷存系統備援機制。
2. 台灣總公司與東莞廠 SD-WIN 專線架設完畢。
3. 定期監控系統的更新狀態，修補已知漏洞，確保所有系統保持最新狀態。
4. 每年年底前定期複核使用者權限，對於調職及離職員工，修正或刪除權限，以防止資料未授權的存取。

5. 使用自動更新防毒系統，隨時監視病毒事件並加以排除。
6. 不定期宣導資安教育訓練

軟體漏洞是現代威脅環境中的一大挑戰，也是惡意攻擊者入侵統的最常見的途徑之一，但通過及時更新軟體，可以顯著降低潛在的風險，確保系統和資料的安全，這是維護數任位安全的關鍵步驟之一。許多軟體並沒有自動更新功能，以 7-ZIP 的軟體漏洞，也引發資安界的關注。籍由此事件，我司宣導不要自行安裝未經公司授權的軟體，避免成為攻擊者的目標。