

台灣圓點奈米技術股份有限公司
Taiwan Advanced Nanotech Inc

資訊安全風險管理



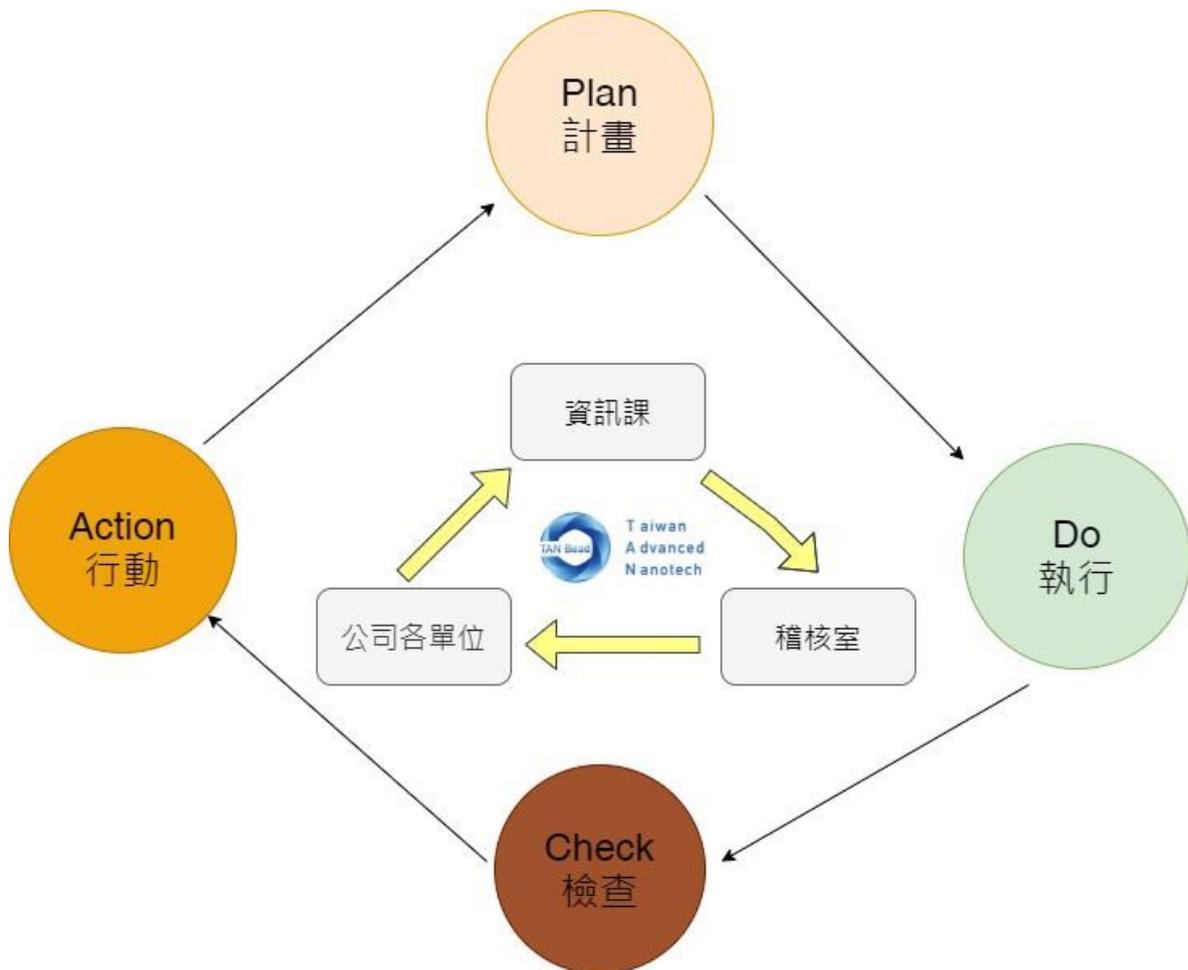
資訊安全風險管理

本公司持續部署 IT 相關系統，為了維護公司治理與降低營運風險，企業必需發展完整資訊安全措施，保護公司重要資訊資產，以追求永續經營的目的。面對新興科技與商業模式轉變，帶來的新型態犯罪的挑戰，公司堅持保護客戶的重要智慧資產，強化專案執行可靠與品質，以提升客戶信賴。並且符合業主要求或法令規定，如營業秘密法、個人資料保護法、資通安全管理法等。

● 資訊安全風險管理架構

公司資訊安全之權責單位為資訊部，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。

本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫及追蹤改善成效，並定期呈報董事會，以降低內部資安風險。組織運作模式-採 PDCA (Plan-Do-Check-Action) 循環式管理，確保可靠度目標之達成且持續改善。



● 資訊安全政策

為貫徹本公司各項資訊管理制度能有效運作執行，並維護重要資訊系統的安全，以確保資訊系統、設備網路之安全維運，達到永續經營目的。

1. 保護個人及機關資訊的機密性、完整性及可用性。
2. 保護各項資訊系統的安全，避免未經授權者非法取得。
3. 建立可靠之資訊環境，並建立異地備援及緊急應變處理機制。
4. 加強各項資訊安全政策宣導及資訊系統教育訓練
5. 建立有效安全防護措施，避免資訊遭誤用或人為破壞，並防止超出授權範圍之使用。
6. 建立各項資訊業務之查詢及溝通管道。
7. 避免侵權，全體員工嚴禁安裝一切公司無購買之授權資訊軟體。

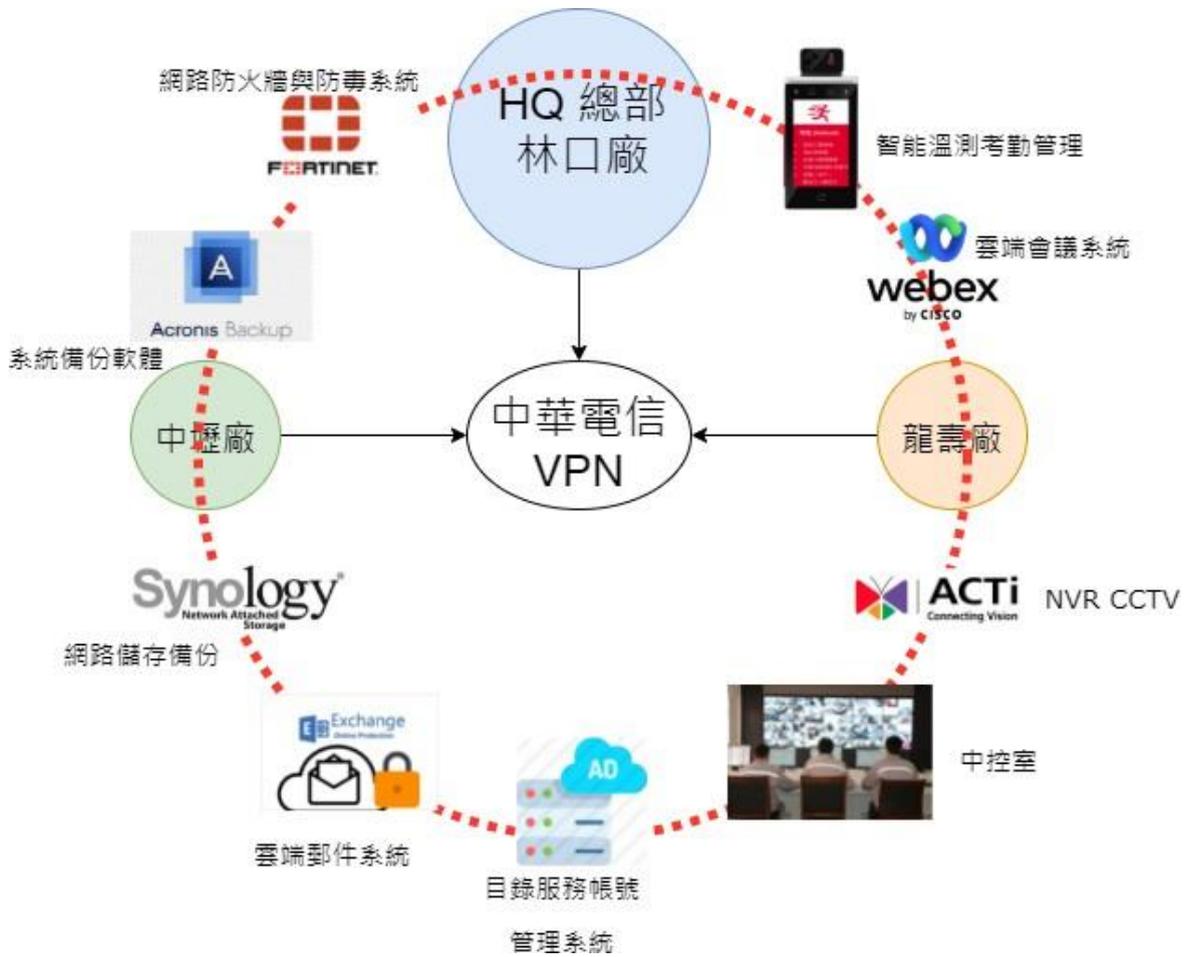
● 本公司之資訊安全管理措施

近年資安風險頻傳，本公司以嚴謹負責的態度建立一套全方位之防護系統，其範圍包含最低層之員工電腦至最高層之對外網路端點。但由於第三方網路攻擊方式不斷的變化與推陳出新，防護系統並無法保證能永遠不遭受外來之網路攻擊與侵入風險，此風險或能導致公司機密外洩，或遭病毒勒索軟體之騷擾，或干擾公司生產營運造成營業損失。

針對上述風險，本公司採取以下必要之管理措施：

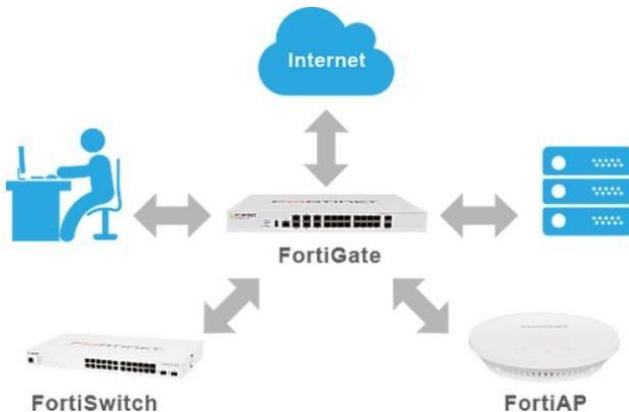
1. 制訂相關資訊安全措施辦法，並全面性追蹤檢討以補既有防護系統之不足。
2. 定期檢視現有資安設備達最佳防護狀態。
3. 與專業第三方服務廠商簽訂維護運作合約，定期維護設備及更新防護系統資料。
4. 定期實施災難復原計畫，透過演練以期縮短風險時間，降低營運損失。

圓點奈米面對各項可能的資安威脅，為降低風險發生的機率與影響，提升公司持續營運能力，透過風險評鑑與資安稽核作業，釐清高風險事項並進行管理，以降低資訊風險發生的可能性與衝擊、並導入科技解決方案與強化資安教育訓練，多管齊下做好資訊安全的管理機制，減少威脅及進行風險管控。



防駭守門員 PLUS

幫您的網路防護強力把關，遏阻勒索病毒、釣魚網站與惡意連結攻擊，可幫助電腦及手機防駭，為您阻擋有害連線，建立安全的網路防護罩，打造安心的上網環境。



資安鐵三角-強大的功能

- 網路拓模圖及流量可視化
- 快速查詢設備資訊
- 有線 / 無線環境均可做 Layer 2 隔離
- IOCs 威脅自動隔離
- 有線 / 無線網路統一接入管理
- 內網 / 外網資安全防禦
- 架構統一彈性擴充

● 資訊安全所投入之資源

資 安 對 應 措 施		
外部威脅	內部系統潛在風險、中毒管理	<ul style="list-style-type: none"> ● 對外主機弱點檢測 ● 病毒防護與惡意程式偵測 ● 電子郵社交工程演練及資安訓練資料
資料安全性	系統與個人資料安全維護措施	<ul style="list-style-type: none"> ● 禁止使用未授權之非法軟體 ● 合法軟體授權與使用管理 ● 資料備份及災害還原並定期演練 ● 定期備份個人重要資料至 NAS
權限管理	人員帳號、權限管理、系統操作行為管理	<ul style="list-style-type: none"> ● 人員帳號權限管理與審核 ● 各系統實施多層次權限及密碼管制 ● 內、外部網域、網路使用管制
存取控制	人員存取內外部系統及資料行為記錄	<ul style="list-style-type: none"> ● 封鎖 USB 儲存裝置 ● 文件檔案夾採取不同單位權限設定 ● 針對個別使用者文件操作行為紀錄
設備安全與可靠度	資訊機房保全及環境安全維護，系統可用與服務中斷時之處置措施	<ul style="list-style-type: none"> ● 資訊機房進出安全管制 ● UPS 電源、空調備援及消防安全 ● 設備、網路可用性監測及通報

圓點奈米每年持續投入資源於資訊安全相關事務上，資訊安全相關設備的投入有防毒系統、垃圾郵件過濾、備份系統、防火牆、VPN 網路等來強化資安防禦，並持續改善資安管理制度與教育訓練等，從管理面到技術面來增加資訊安全能力。



TANBEAD

台灣圓點奈米技術股份有限公司