大田精密工業股份有限公司

資通安全管理

一、資通安全風險管理架構、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。

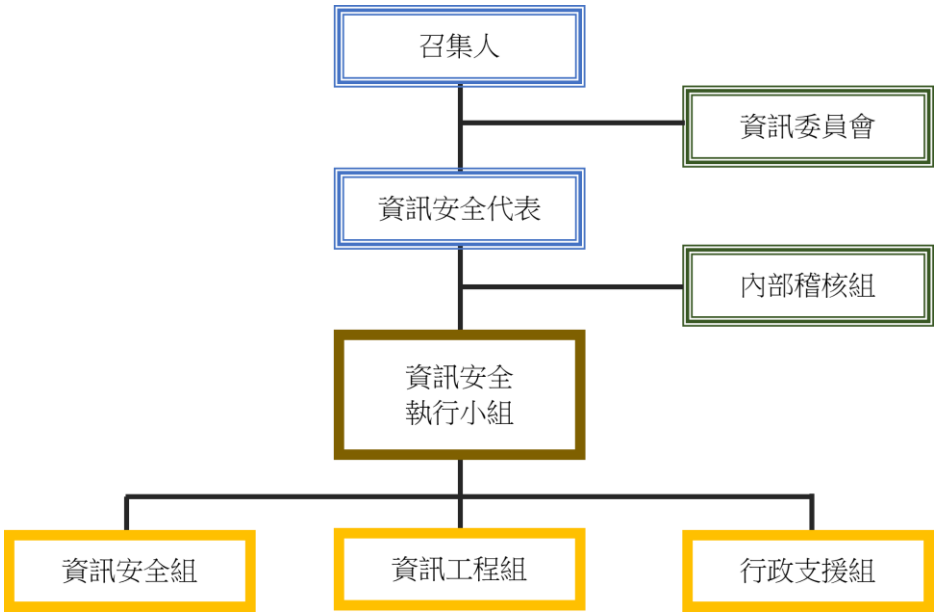
1. 資通安全風險管理架構

(1)企業資訊安全管理組織

大田精密工業股份有限公司設立「企業資訊安全組織」，下轄資訊相關單位，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，並由企業資訊安全組織最高主管彙報資安管理成效、資安相關議題及方向。

為執行企業資訊安全組織訂定的資安策略，確保內部遵循資安相關準則、程序與法規，由召集人指派資訊技術負責人擔任資訊安全代表，並由各部主管擔任委員，視必要性召開會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

(2)大田精密工業股份有限公司企業資訊安全組織架構

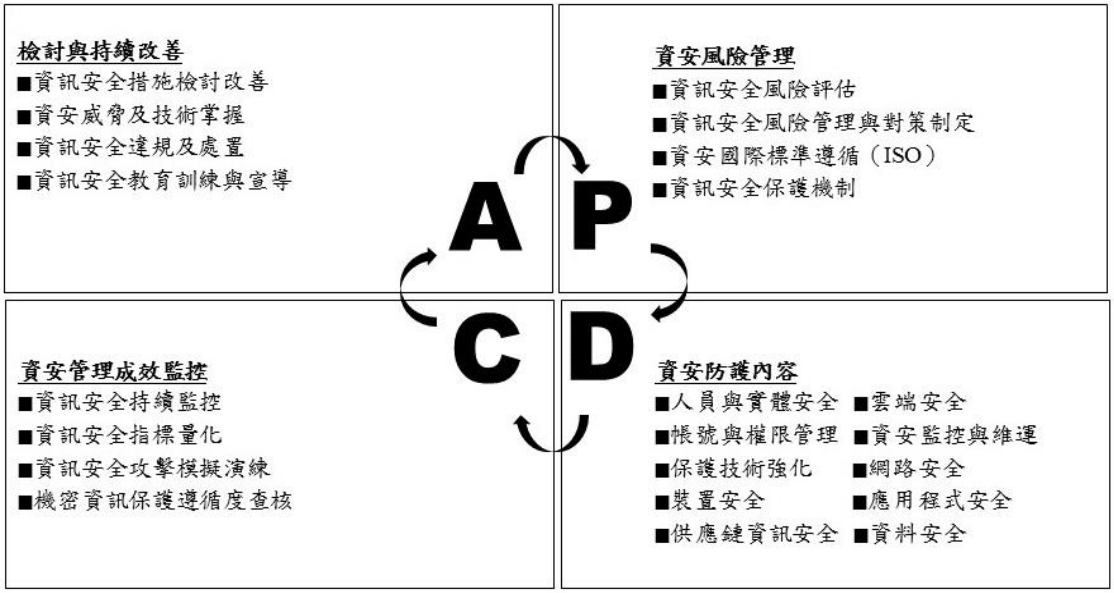


2. 資通安全政策

(1)企業資訊安全管理策略與架構

大田精密工業股份有限公司為有效落實資安管理，透過涵蓋台灣廠區與海外子公司資訊單位，藉由每週召開例行會議即時反應資安議題，並依持續改善、追蹤原則，按規畫、執行、查核與行動(PDCA)的管理循環機制，適時調整資訊安全政策適用性與保護措施。「規畫階段」著重資安風險管理，從系統面、技術面、程序面尋求降低企業資安威脅的方法，建立符合客戶需求、高規格的資訊保護服務。「執行階段」則建構多層資安防護，持續導入新資安防禦技術，將資安控管機制整合內化於軟硬體維運、供應鏈資安管理等平日作業流程，並系統化監控資訊安全，維護重要資產的機密性、完整性及可用性。「查核階段」積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析。「行動階段」則以檢討與持續改善為本，落實監督與稽核，確保資安規範持續有效性；不定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作業，確保公司重要機密資訊不外洩。

(2)企業資訊安全風險管理與持續改善架構



(3)具體管理方案

A.分層資安防護

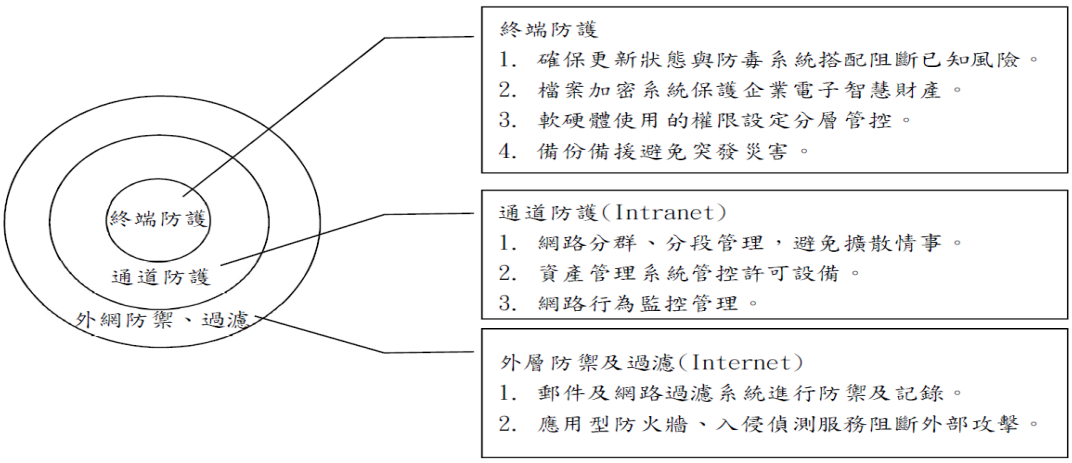
終端防護層	● 機台入廠不連網及掃毒機制，防止內含惡意軟體的機台進入公司。 ● 端點防毒措施，防止及強化惡意軟體行為。 ● 郵件外寄控管。 ● 規劃文件及資料加密控管及有效追蹤。 ● 使用資訊保護工具，藉由分類、帳密保護資料。
通道防護層	● 制定應用程式安全測試及自檢表。 ● 持續強化應用程式安全控管機制。
外網防禦、過濾層	● 導入先進技術執行電腦掃描及系統與軟體更新。 ● 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨廠區擴散。

B.檢討與持續改善

教育訓練與宣導	1. 指派資安人員積極參與資安訓練課程。 2. 加強員工對郵件社交工程攻擊的警覺性，執行釣魚郵件防禦偵測。 3. 不定期舉辦資安教育訓練，提升員工資安意識。

C.資安成效監控

資安評估	● 委託外部專家、廠商提供新知及先進產品測試。 ● 持續搜集威脅情資，進行風險分析，進階強化資安管理體制。



(4)投入資通安全管理之資源

制定「資訊安全管理辦法」與相關作業細則，據以執行相關工作計畫，持續完善防護。如建置應用層防火牆、惡意郵件過濾系統、員工上網防護、作業系統更新、防毒軟體佈署、電子資料存放平台…等。而資訊安全為企業營運上持續不斷改善之項目，亦為企業全體同仁共同認知，其資源之投入。除研究相關最新技術外，近年導入應用型防火牆、網路資安艦隊服務，用以防禦更新、更高層次的網路攻擊行為；另也積極建置保護我司及其客戶、供應商資產之方案。

(5)資通安全風險與管理措施：

大田精密工業股份有限公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造、營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵公司內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，系統可能會失去公司重要的資料，生產線也可能因此停擺。大田精密工業股份有限公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業。

管理措施：

A. 另針對主要關鍵系統及關鍵資料，除高可用性的系統功能建置及備援負載外，也進行資料備份機制，以維持公司營運不中斷。

B. 關鍵資訊系統公司皆指定團隊及專人進行保護及管理。

C. 每年定期稽核，其內容含營業機密、政府法令規章、生產製令、資訊系統等要求。並能與時俱進調整制度及管控措施，以符合要求及業務需求。目前資訊系統皆有持續稽核改善，降低營運衝擊，且能於風險發生時，迅速恢復業務，降低客戶損失及維持公司運維。

二、列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：本公司於民國108年、109年及110年級截至年報刊印日止，未發生任何衝擊公司營運的重大網路攻擊事件。

三、本公司依「公開發行公司建立內部控制制度處理準則」第九條之一規定，於111年3月21日申報資安主管及資安人員資料。

四、執行情形

1.111年11月1日提報董事會資訊安全管理架構暨資訊安全政策及具體管理方案。

2.112年11月9日提報董事會資訊安全管理架構暨資訊安全政策及具體管理方案。