資訊安全

為了維護公司股東與客戶最大權益，南亞科技積極推動資訊安全相關制度及防護系統，過去公司 7 年已投入資安領域超過十億新臺幣以上之資金，並成立了資訊安全委員會，由總經理親自督導，並持續精進本公司之資訊安全管理，恪守相關法規要求，偕同全體員工及供應鏈夥伴，共同確保資訊資產的機密性、完整性及可用性，以保障本公司客戶、股東、員工及供應商之權益，並善盡社會責任。 資訊安全政策

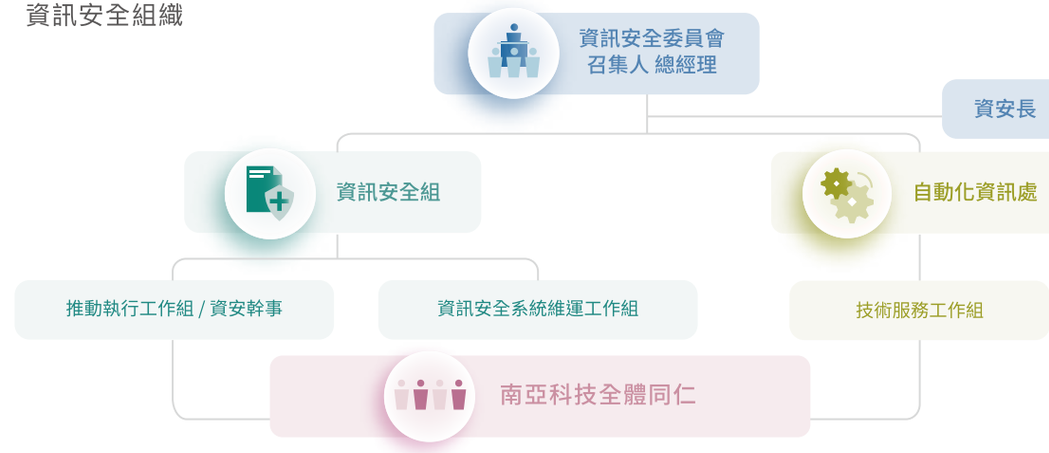
我們在 DRAM 記憶體領域深耕數十年，深知 DRAM 製程與產品研發的挑戰、先進製程開發、生產的 Know-How 與智慧財產權保護的重要性，所以我們相當重視資訊安全，透過加強資安防護措施及員工對資安意識的認知與重視，避免機敏技術資料外流，以維持公司持續研發能量及核心競爭能力，如此才能夠保護公司的長遠利益及同仁的工作權益。

南亞科技 2022 年再度通過 ISO 27001 三年一次的資訊安全驗證，驗證範圍擴大至全廠區導入函蓋率達 100%，並於 2024 年度維持證書有效性，彰顯南亞科技對資訊安全管理制度的重視，同時也符合國際標準。

為更進一步的落實資訊安全管理，南亞科技成立跨部門之資訊安全委員會，由總經理擔任召集人，並指派數名一級主管擔任委員，及指派一名委員擔任資安長職務 (執行秘書)，成員分別為資安長 (黃晏昌資深處長)、品保處、法務及智慧財產處、人力資源處及自動化資訊處。資訊安全委員會每週召開，主要負責資訊安全政策、目標及相關規範之規劃擬定、核准及督導，並每季向董事會成員報告資訊安全管理系統的運作之成效及更進一步強化的機會。同時，我們的 4 位執行董事 (李培瑛 總經理、蘇林慶 執行副總、吳志祥 副總及莊達人 副總) 積極參與公司資訊安全季會以及每年一次的資訊安全管理審查會議，確保其管理之有效性與效益。

本公司配合資通安全管理法實施，南亞科技比照資通安全責任等級 A 級之公務機關應辦事項，及目前已取得有效資通安全專業證照，包含 EC-Council CCISO (Certified Chief Information Security Officer，資安長)、CISSP 認證資訊系統安全專家、EC-Council ECSA (Certified Security Analyst，資安分析專家)、EC-Council CEH (Certificated Ethical Hacker 駭客技術專家)、CompTIA Security+ 國際網路資安、EC-Council CND 網路防禦專家、EC-Council CPENT 滲透測試專家、EC-Council CASE .NET 應用程式安全工程師、及 ISO/IEC 27001:2013 Information Security Management System(ISMS) Lead Auditor(ISMS 主導稽核員) 等，提升南亞科技資安人力專業職能以及執行效率。

資訊安全組織



南亞科技資訊安全管理改善措施里程碑

2017	● 針對同業挖角員工導致不當取得公司機密及商業敏感資料之風險，設置資訊安全組，負責規劃、執行、稽核及改善資訊安全管理。
2019	● 首次取得ISO27001資訊安全管理系統國際標準證書。 ● 因應國內外資安攻擊事件頻傳，及攻擊手法層出不窮，持續發展外部駭客防護策略與縱深防禦方案。
2022	● 再度通過ISO27001三年一次的資訊安全管理系統標準驗證，驗證範圍擴大至全廠區導入。 ● 建置OT(Facility)資安防護系統，落實弱點管理並建置監控及應變機制。 ● 執行主要下游外包廠商進行ISMS資安管理查核作業，以持續提升供應鏈資安的有效性。
2023	● 將供應商分類與分級，針對關鍵高風險供應商進行風險管理及稽核改善。
2024	● (Facility/FAB)OT資安防護；強化工控設備可視度提升，掌握廠域及機台設備正常連線行為，以降低未經授權的外來設備曝險。 ● 資訊安全自動化聯防與回應系統全日監控超過38萬次的活動，自動阻擋可疑IP來源，提高威脅偵測與資安事件應變能力。 ● 改善供應鏈資訊安全管理，選定供應商Scope(2024年共137家)，執行SAQ及第三方風險評估，完成關鍵高風險供應商稽核及改善。 ● 依循NIST標準的網絡安全框架模板，並透過第三方自評資安風險評分工具來分析、評估多面向的合規性，以做好資訊安全管理。

一．資訊安全管理主要做法與執行成果

南亞科技為落實資訊安全政策，確保資訊的機密性、完整性及可用性，以保障本公司客戶、股東、員工及供應商之權益，2024 年執行成果詳如說明：

01 強化資訊安全，建立縱深防禦

- 由機敏資料加密、端點防護與網路閘道防護，搭配網路存取管制、文件輸出管理與電子郵件防護等機制，並針對資安管制品導入金屬探測門，以防範由外而內的網路攻擊與由內而外的洩密行為。
- 強化端點安全防護：安裝防毒軟體、更新原廠安全性修補程式、控管USB存取及建立備援機制以強化系統防禦降低系統漏洞風險。
- 防護外部攻擊威脅：設置資安防護系統、隔離上網及檔案無害化機制，防範電腦病毒或惡意程式影響資訊系統服務或窺探機密資料，及透過社交工程竊取機密資料。
- (Facility/FAB)OT資安防護；強化工控設備可視度提升，掌握廠域及機台設備正常連線行為，以降低未經授權的外來設備曝險。
- 資訊安全自動化聯防與回應系統年度監控超過38萬次的活動，自動阻擋可疑IP來源，提高威脅偵測與資安事件應變能力。

02 建立實體安全防護

- 訂定「公司機密管理辦法」進出辦公區及廠區皆設有金屬探測門，物品攜出入皆須隨人員通過金屬探測門，及公司機密資訊未經授權，不得對他人揭露，亦訂定相關評核機制。
- 建立門禁控管、登入系統的身分驗證、密碼控管、存取授權及定期進行弱點掃描等稽核機制。

03 品質管理及法令法規遵循

- 2022年再度通過ISO 27001三年一次的資訊安全驗證，至今擴大至全廠區導入函蓋率達100%，並於2024年度通過第三稽核單位台灣檢驗科技股份有限公司(SGS)認證以維持證書有效性，彰顯南亞科技對資訊安全管理制度的重視，同時也符合國際標準。 ISO 27001 證書
- 每年檢視資安防護措施及規章，關注資安議題及擬訂因應計畫，以確保其適當性及有效性，並於ISO管理審查會議進行報告。
- 本公司一向重視資訊安全及個人資料保護，並保障客戶權益及善盡個人資料保護責任，針對個人資料存取權限加以區隔與管控，並設有傳輸加密保護機制，以避免未經授權外洩之事件發生。
- 依循NIST標準的網絡安全框架模板，並透過第三方自評資安風險評分工具來分析、評估多面向的合規性，以做好資訊安全管理。

04 資安意識教育訓練

- 社交工程演練，導入業界知名釣魚郵件測試工具，每季進行多次社交工程偽裝寄送擬真釣魚郵件演練並設定演練目標，並對點擊郵件連結及開啟附件之員工加強教育訓練，同時亦訂定相關評核機制，藉使全體員工重視該項作業，以強化資安防護意識，全年累計共執行8次，演練人數超過2.9萬人次，海外子公司超過1,331人次。
- 每年定期對員工及新進人員進行資訊安全教育訓練，強化員工的資安風險意識。
- 人才專業化培育；招募及培育資訊人員專業及跨域整合能力，取得國際專業證照提升人員本職學能與擴展領域。

05 營運持續

- 由於資安事件層出不窮，本公司訂有「資訊安全事故通報及管理辦法」做為資安事件通報與管理，每年不定期針對資安事件應變處理進行演練。
- 遵循「上市上櫃公司資通安全管控指引」製定資安事件等級及內外部通報對象與流程，及訂有利害關係人受駭之威脅情資應變處理程序，避免營運受影響。
- 本公司針對關鍵營運流程影響嚴重程度進行風險評估與辨識，並做為災難復原演練頻率之依據。
- 定義辦公區、研發設計與技術開發等資訊系統可用性目標，訂定年度目標停止服務為每年≤1次及<24小時，2024年資訊系統未有發生服務中斷事件。

06 供應鏈安全防護

- 除了公司本身，亦擴展至供應鏈的資安防護，設備入廠時必須通過安全性檢查，方得上線使用，更與廠商及其入廠人員簽署資安條款，以防範有心人士藉由供應鏈關係進行攻擊。
- 2024年執行主要下游外包廠商進行ISMS資安管理查核作業，發現潛在不合格事項，經由適當的矯正及預防措施處理，以確保供應鏈符合本公司資安的要求。
- 2024年執行透過自我評量問卷(SAQ)及安全計分卡(Security Scorecard)，將供應商分類與分級，針對關鍵高風險供應商進行風險管理及稽核改善。

07 探討資安事件與駭客攻擊手法

- 積極參與台灣電腦網路危機處理暨協調中心(TWCERT/CC)情資分享，以加速了解駭客攻擊手法等情資，提早採取防護及應變措施。
- 委由第三方定期每年執行紅隊演練，針對本公司資安防護，檢測系統漏洞及弱點，以及早發現並加以改善修正。
- 主動參加台灣電腦網路危機處理暨協調中心(TWCERT/CC)辦理2024年度企業資安演練，強化企業的資安事件應變能力，提升整體資安防護量能。

二．營運持續計畫（BCP）

・資安事件演練作業：本公司每年不定期針對資安事件樣態進行應變處理演練作業，包含電腦受駭及官方網站遭受 DDoS 攻擊等，以驗證資安事故通報及應變程序時效性。

・資訊系統營運持續作業：因應各部門資訊系統架構有所不同，我們針對各系統架構對關鍵營運流程影響嚴重程度進行風險評估與辨識，定義其嚴重層級 (Degree) 分類，做為災難復原演練頻率之依據，由重要至輕微分為三級 (Degree 1~3)，各層級說明如下：

嚴重層級分類與復原演練週期關係表

Degree 1	Degree 2	Degree 3
此系統停止運轉將造成主要機能無法提供服務。	此系統停止運轉將造成次要機能無法提供服務。	此系統停止運轉不會影響所提供之服務，或此系統所提供之服務可藉由其餘補償措施維持運作。
復原演練週期 一年	復原演練週期 二年	復原演練週期 可不演練

復原演練週期亦搭配嚴重層級有所區分 (每一年、每二年、可不演練)，各部門將負責之維運系統等級登錄於「資訊系統嚴重層級分類」之文件清單中。所有 Degree 1 系統皆有多重備援機制，分別放置於不同建築物的不同機房，重要生產資料皆以加密方式進行異地備份，並依資訊系統災難復原計畫進行演練，以確保系統正常運作。2024 年需執行演練系統共有 12 個，實際演練系統完成 12 個，演練系統達成率 100%。各資訊系統管理單位於重大異常發生時，依照「資訊系統應變措施計劃表」定義之應變流程，通知應變單位執行因應措施。

三．資訊安全認知教育訓練與執行成果

資訊安全組指派專人擔任，組員由各部門資安幹事擔任，工作任務包含配合實施資訊安全認知教育訓練、相關管理規範制修定、資訊資產風險評鑑作業等作業。

在資訊安全認知教育訓練部分，南亞科技投入許多資源，希望針對全體員工提升資安防護意識與凝聚共識，每月資安月會針對資安幹事 進行宣導，每季資安季會則針對一級以上主管報告績效評比結果，每季亦進行社交工程演練，每年舉辦資安月活動，及為了深植對機密資訊管理的文化，全體員工每年皆需完成「公司機密管理辦法」之線上指定閱讀課程。2024 年辦理課程及時數詳如下表：

訓練類別	資訊安全認知教育訓練課程	對象	時數
全員指定閱讀	公司機密管理辦法	全體員工	1,827
	認識 BEC 商業電子郵件詐騙 (I)	全體員工	1,822
	如何防止 BEC 詐騙 (II)	全體員工	1,832
	URL 辨識訓練	全體員工	1,799
新進人員資安教育	做好資訊安全管理 (I)	新進人員 (一週內)	665
	做好資訊安全管理 (II)	新進人員 (六個月內)	516
社交工程教育訓練	社交工程演練	全體員工 (不含 TA)	2,528
	社交工程教育訓練	演練點擊員工	52
資安講座 (外聘講師)	資安護城河：守護您的數位世界	資安幹事、資訊安全組	78
	防護數位世界的大門：了解 ISO 27001	單位主管、資訊安全組	79
	Entra ID 雲端身分保護功能 & 效益	資安幹事、資訊安全組	27
	營業秘密專題演講	單位主管、資訊安全組、供應鏈廠商	130
	資安研討會零信任主題講座	單位主管、資訊安全組、供應鏈廠商	112
內部稽核員訓練	ISO 27001 內部稽核員訓練	資安幹事	118
資安月活動	資訊安全管理問答題測驗	全體員工	1,822
全年度資訊安全認知教育訓練總時數			13,406

四．資訊安全目標達成情形

本公司了解資訊安全持續面臨威脅及風險，公司全面佈署適當的資安防護機制，2024 年通過第三方稽核無重大缺失，亦無客戶資訊洩漏及罰款等重大資安事件發生，詳如下表：

項目	統計
違反資安或網路安全事件 (件)	0 件
資料洩漏事件 (件)	0 件
涉及顧客個人資料之資安違反事件 (件)	0 件
因資料洩漏而受影響的顧客與員工人數 (人)	0 次
因資訊安全或網路安全相關事件遭判罰之罰款金額 (新臺幣元)	0 元

五．供應鏈資訊安全

為推廣供應鏈資訊安全，本公司依「重要性」、「風險性」、「年度採購金額」、「永續發展」等因子，篩選出納入管控的關注第一階供應商、設備廠商、外包廠及系統整合廠商（2024 年共 140 家），搭配第三方資安風險評估 (分數需達 80 分或等級 B 以上) 及南亞科技資安自主評鑑 (分數 85 分以上)，未達標準將納入關鍵高風險供應商範圍，南亞科技將進行現場稽核及後續輔導追蹤持續改善，並要求於採購合約中簽訂資安條款及「遵守資訊安全政策承諾書」以確保資訊安全。

關鍵供應商

依「重要性」、「風險性」、「年度採購金額」、「永續發展」等因子，篩選出納入管控的關注第一階供應商、設備廠商、外包廠及系統整合廠商（共140家）

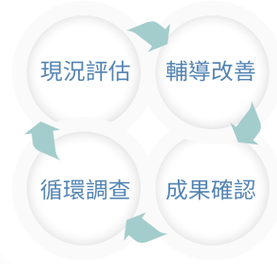
第三方風險評估

由供應商自行提供第三方資安風險評估工具之資安風險評級或分數，並須達到等級B或80分以上

SAQ自我資安評鑑

依照SAQ調查結果、資安認證及重大資安事故紀錄判定風險（85分以上）

供應鏈資安評鑑流程



2024 年，完成評鑑的供應商家數已擴增至 140 家，相較去年增加了 164%，以資安個別輔導、教育訓練、Security Score Card 要求及現場實地稽核等方式，持續陪伴供應商夥伴精進營運資訊安全管理，也逐步要求供應商通過國際認證 (如 :ISO 27001)，目前取得認證家數占比 33%。2024 年為提升供應商對於資訊安全的意識，邀請供應商參加南亞科技資安月活動 - 零信任「永不信任、持續驗證」研討會，透過行業領袖和資深專家進行分享與交流，探討如何透過零信任架構提升供應鏈安全，確保我們共同的業務數據和資產免受現代化威脅的侵害，活動共計 17 家供應商共 37 位人員參與。