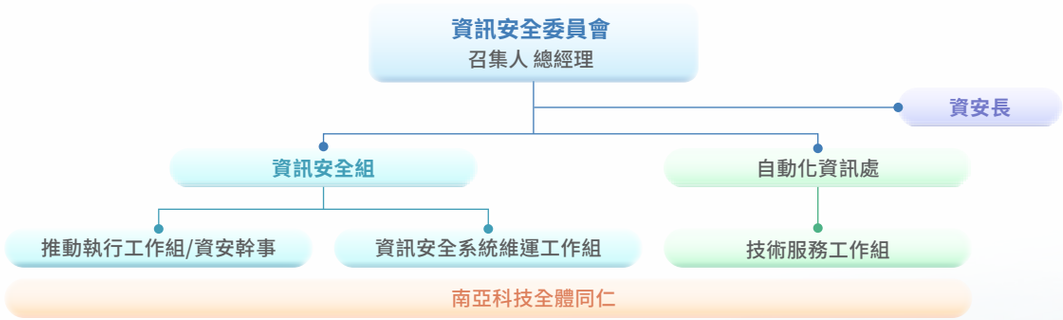
8.3 資訊安全

為維護股東與客戶之最大權益，南亞科技積極推動資訊安全管理制度與防護系統。過去八年，公司於資安領域累計投入逾新臺幣十億元，並成立資訊安全委員會，由總經理親自督導，持續精進資訊安全管理作為。公司恪守相關法規要求，並攜手全體員工與供應鏈夥伴，共同確保資訊資產之機密性、完整性與可用性，保障客戶、股東、員工及供應商之權益，善盡企業社會責任。資訊安全政策

南亞科技深耕 DRAM 記憶體領域數十年，深知先進製程開發、產品研發與量產過程中，製程 Know-how 與智慧財產保護之關鍵性。因此，公司高度重視資訊安全，透過強化資安防護措施與提升員工資安意識，降低機敏技術資料外流風險，以維持持續研發能量與核心競爭力，進而保障公司長期利益與同仁工作權益。

為進一步落實資訊安全治理，公司設立跨部門資訊安全委員會，由總經理擔任召集人，並由多位一級主管擔任委員，另指派一名委員兼任資安長 (執行秘書)。委員會成員包含：資安長黃晏昌協理、品保處、法務及智慧財產處、人力資源處與自動化資訊處。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、核准與督導，並每季向董事會報告資訊安全管理系統運作成效及持續強化機會。

此外，四位執行董事 (李培瑛董事、蘇林慶董事、吳志祥董事及莊達人董事) 積極參與公司資訊安全季會及每年一次之資訊安全管理審查會議，以確保資訊安全管理制度之有效性與效益。



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，2025 年執行成果詳如說明：

01 資訊安全品質管理及法令法規遵循

(1) 2025 年再度通過第三稽核單位台灣檢驗科技股份有限公司 (SGS) 認證 ISO 27001 三年一次的資訊安全驗證，及至今擴大至全廠區導入函蓋率達 100%，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

(2) 依據 ISO 27001 已建立資訊安全目標達成狀況 ，共計 13 項量化型指標。

(3) 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。

(4) 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。

02 強化資訊安全縱深防禦

(1) 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。

(2) 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。

(3) 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。

(4) (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。

(5) 資訊安全自動化聯防與回應系統年度監控超過 52 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。

03 強化資訊資產防護與韌性

本公司視資訊資產為核心競爭力，透過嚴密的資產分級、存取控管與維運技術，建構具備高度韌性的防禦體系，確保業務連續性並守護客戶信任。

(1) 建立完善之資訊資產管理程序，定期進行軟硬體資產盤點與風險評估。針對關鍵數據與個人資料，採用加密儲存與傳輸技術，並透過資料外洩系統防止未授權之資料外流，確保客戶隱私與公司智慧財產權之安全。

(2) 僅授予員工執行工作所需的最低限度權限，嚴格執行『最小權限賦予原則』，確保離職或職務異動人員之權限即時回收，並每半年針對高權限帳號進行查核，杜絕非法存取風險。

(3) 應用程式安全方面；本公司確保伺服器與作業系統定期更新補丁，並執行異地備份以保障營運持續性。針對自主開發之應用程式，導入 SSDLC 安全開發流程，於上線前通過弱點掃描與滲透測試，確保軟體無重大安全漏洞。

04 建立實體安全防護

(1) 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。

(2) 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。

05 營運持續與資安事件應變措施

(1) 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，並遵循「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。

(2) 每年不定期針對資安事件樣態進行應變處理演練作業，2025 年度協同下游委外廠商進行資料外洩危機通報程序，及訂定利害關係人受駭侵緊急應變程序，以驗證應變程序時效性。

(3) 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。

(4) 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，2025 年資訊系統未有發生服務中斷事件。

06 探討資安事件與駭客攻擊手法

(1) 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。

(2) 持續加強內外資安防護並與調查局緊密合作進行情資交換。

(3) 每年參與企業紅隊演練，2025 年度無重大缺失，相關發現皆已完成改善，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。

(4) 為確保資通安全與企業機密完整性，本公司明確禁止使用未經授權之雲端生成式 AI 工具，並同步導入 AI 大語言模型系統性風險評估機制，建構全方位防護措施。此外，已正式頒布《CNDCI-0568 生成式 AI 開發管理辦法》，針對技術開發與應用落實制度化管理，落實數位治理責任。

07 資安意識教育訓練

(1) 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。

(2) 不定期針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。

(3) 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，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，及目前已取得資通安全專業證照 (包含 EC-Council CCISO (Certified Chief Information Security Officer, 資　安　長)、ISC2 CISSP (Certified Information Systems Security Professional, 資訊安全系統專家)、EC-Council CPENT (Certificated Penetration Test Professional, 滲透測試專家)、EC-Council CND (Certified Network Defender, 網路防禦專家)、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。

08 供應鏈資訊安全 (政策及原則)

(1) 本公司秉持『風險導向』管理方針，制定相關供應商資安管理規範，要求合作夥伴遵循與本公司同等之防護標準。針對核心系統及數據服務商，我們於採購合約中明文納入資安稽核權。

(2) 深化供應鏈資安管理，建立 SAQ (Self-Assessment Questionnaire) 供應商自評問卷，讓供應商檢視自身合規狀況，並作為企業初步篩選或分級的依據。搭配獨立第三方 SSC (Social/Security Compliance) 稽核，以確保供應商在 SAQ 中的回覆與實際情況相符。

(3) 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。

(4) 2025 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。

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。2025 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
全員資安意識宣導	資訊安全政策閱讀	全體員工	911
	公司機密管理辦法	全體員工	1,866
新人教育訓練	做好資訊安全管理 (I)	新進員工	894
	做好資訊安全管理 (II)	新進員工	868
社交工程教育訓練	社交工程演練	全體員工 (不含 TA)	2,520
	常見社交工程攻擊手法解析與識別	演練點擊員工	5
	URL 辨識訓練	演練點擊員工	9
	資訊安全補充課程 (Emails_in_Real_Life)	近兩年新進員工	347
資安講座 (外聘講師)	跨域攻擊防禦：從端點到身份再到雲端	資安幹事、資訊安全組	123
	資通安全暨新型態網路詐騙案例分享	單位主管、資訊安全組	128
	資安研討會主題講座	資安幹事、資訊安全組	125
資安管理專業訓練	應用系統安全開發設計指引	系統開發維運人員	41
其他	資訊安全管理問答題測驗	全體員工	1,833
合計			11,467

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，2025 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

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 (2025 年共 150 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。

2025 年，完成評鑑的供應商家數已擴增至 150 家，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 37%。2025 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「安無所不在 共築安全營運防線」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 26 家供應商共 46 位人員參與。

共150家

依「重要性」、「風險性」、「年度採購金額」、「永續發展」等因子，篩選出須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

等級B或80分以上

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

85分↑

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↑)