

8.3 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 6 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，整體資安運作已上軌道，並持續改善精進以因應外在局勢威脅，確保公司營運順暢並取得公司股東與客戶的信賴。

資訊安全政策

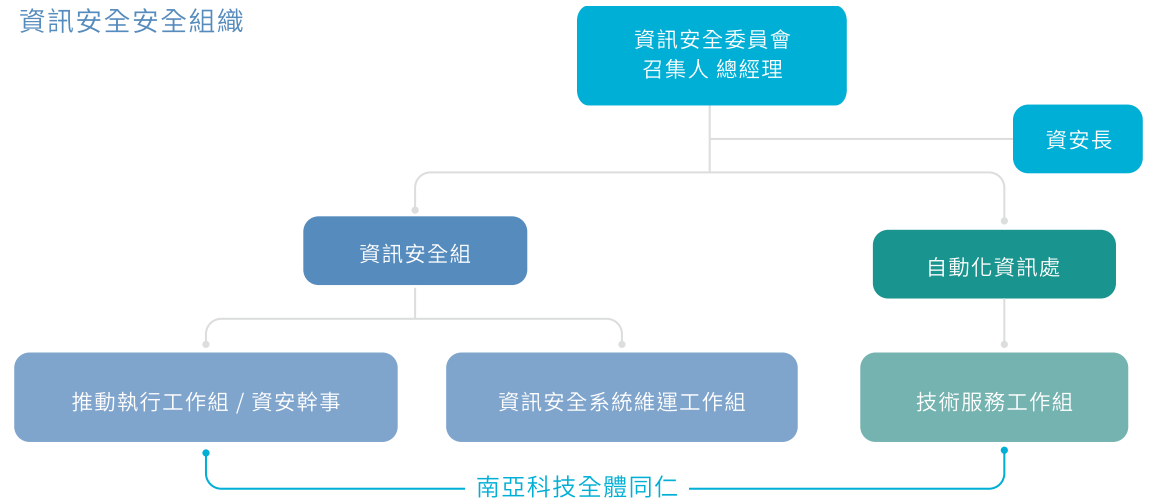
我們在 DRAM 記憶體領域深耕數十年，深知 DRAM 製程與產品研發的挑戰、先進製程開發、生產的 Know-How 與智慧財產權保護的重要性，所以我們相當重視資訊安全，透過加強資安防護措施及員工對資安意識的認知與重視，避免機敏技術資料外流，以維持公司持續研發能量及核心競爭能力，如此才能夠保護公司的長遠利益及同仁的工作權益。

南亞科技 2022 年再度通過 ISO 27001 三年一次的資訊安全驗證，驗證範圍由原本六個主要單位，至今擴大至全廠區導入函蓋率達 100%，並於 2023 年度維持證書有效性，彰顯南亞科技對資訊安全管理制度之重視，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）每季皆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。

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)、EC-Council ECSA (Certified Security Analyst, 資安分析專家)、EC-Council CEH (Certificated Ethical Hacker 駭客技術專家)、EC-Council ECIH (Certified Incident Handler 資安危機處理員)、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、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。

資訊安全安全組織



南亞科技資訊安全管理改善措施里程碑



資訊安全管理主要作法與執行成果

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，2023 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。
- ◆ 建置 (Facility/FAB) OT資安防護系統：以提高資產可視性管理，即時監控威脅與加速事件調查與回應。
- ◆ 建置資訊安全自動化聯防與回應系統，提高威脅偵測與資安事件應變能力。



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，驗證範圍由原本六個主要單位，至今擴大至全廠區導入函蓋率達100%，並於2023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。[ISO 27001 相關證書](#)
- ◆ 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。



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。



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2.8萬人次，海外子公司超過700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

- ◆ 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，2023年資訊系統未有發生服務中斷事件。

06 供應鏈安全防護

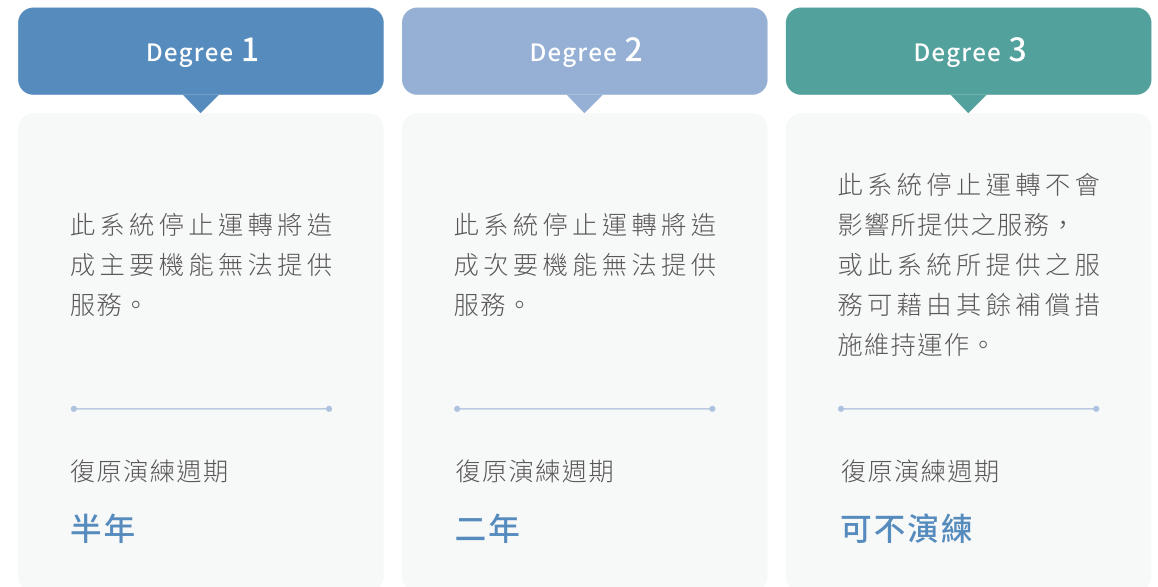
- ◆ 除了公司本身，亦擴展至供應鏈的資安防護，設備入廠時必須通過安全性檢查，方得上線使用，更與廠商及其入廠人員簽署資安條款，以防範有心人士藉由供應鏈關係進行攻擊。
- ◆ 2023年執行主要下游外包廠商進行ISMS資安管理查核作業，發現潛在不合格事項，經由適當的矯正及預防措施處理，以確保供應鏈符合本公司資安的要求。
- ◆ 2023年執行透過自我評量問卷(SAQ)及安全計分卡(Security Scorecard)，將供應商分類與分級，針對關鍵高風險供應商進行風險管理及稽核改善。

07 探討資安事件與駭客攻擊手法

- ◆ 建立自主對外服務系統進行滲透檢查，完成對外21個網站，發現的安全弱點及加以改善。
- ◆ 2022年正式加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，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滲透測試、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2023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。

營運持續計畫

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



復原演練週期亦搭配嚴重層級有所區分 (每半年、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。2023 年需執行演練系統共有 17 個，實際演練系統完成 17 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。

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，工作任務包含配合資訊安全組實施資訊安全認知教育訓練、資訊安全相關文件制定與修改、資訊風險評鑑作業之規劃與執行、協助與配合資訊安全組或其他單位有關資訊安全事務之作業。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。2023 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 (小時)
全員指定閱讀	公司機密管理辦法	全體員工	3,629
新進人員資安教育	做好資訊安全管理 (I)	新進人員 (一週內)	440
	做好資訊安全管理 (II)	新進人員 (六個月內)	570
社交工程教育訓練	社交工程演練	全體員工 (不含 TA)	2,333
	社交工程教育訓練	演練點擊員工	14
資安講座 (外聘講師)	AI 人工智慧應用與資訊安全	資安幹事、資訊安全組	101
	常見的駭侵手法及建議的因應方式	單位主管、資訊安全組	77
內部稽核員訓練	ISO 27001 內部稽核員訓練	資安幹事	90
資安月活動	資訊安全管理問答題測驗	全體員工	1,780
總時數			9,031

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，2023 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

