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 5 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。

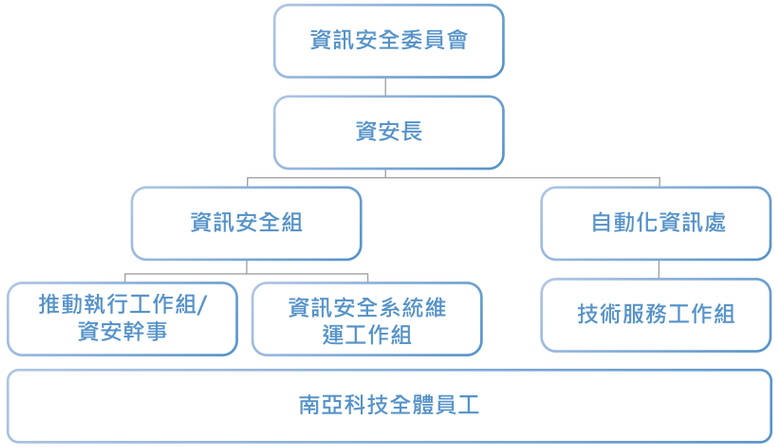
我們在 DRAM 記憶體領域深耕數十年，深知 DRAM 製程與產品研發的挑戰、先進製程開發、生產的 Know-How 與智慧財產權保護的重要性，所以我們相當重視資訊安全，透過加強資安防護措施及員工對資安意識的認知與重視，避免機敏技術資料外流，以維持公司持續研發能量及核心競爭能力，如此才能夠保護公司的長遠利益及同仁的工作權益。

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%，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，並由五位一級主管擔任委員，成員分別為資安長 (牛欣安 特別助理)、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、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。

資訊安全委員會



南亞科技資訊安全管理改善措施

- 2019年本公司取得ISO 27001資安認證，可滿足客戶之要求，並達到國際資安管理系統之標準
- 本公司於「員工手冊」明訂同仁服務守則及保密等相關規定，使員工之行為有所規範
- 本公司同仁任職時所簽署之聘僱承諾書中，即包含承諾於任職期間或離職後，應嚴守保密義務
- 本公司如發現任職或離職員工有違法事件，將依法訴追決不寬待。本公司於106年7月成立資訊安全組至今，已離職員工未有發現違法情事
- 面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，本公司已設有資訊安全組，負責規劃、執行、稽核及改善資訊安全管理
- 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
- 因應國內外資安攻擊事件頻傳，網路駭客透過社交工程、非法入侵或勒索病毒等方式進行破壞與洩密，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
- 2022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
- 2022年建置OT (Facility)資安防護系統，以提高資產可視性，及有效監控與管理機制

南亞科技資訊安全管理主要作法

全面縱深防禦架構
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

建立實體安全防
護建立門禁控管、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

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竊探機密資料，及透過社交工程竊取機密資料

加強資安意識教育訓練
每年定期對員工進行資訊安全教育訓練、社交工程演練及資安測驗，強化員工的資安風險意識

法令法規遵循
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

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

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

探討資安事件與駭客攻擊手法
以預見新興資安威脅之發展與趨勢，於2022年正式加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，以加速了解駭客攻擊手法等情資，俾提早採取防護及應變措施

完成第三方執行滲透測試
交由第三方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

建置OT (Facility)資安防護系統
以提高資產可視性，及有效監控與管理機制

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

營運持續計畫（BCP）

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 **半年**	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。2022 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

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。2022 年辦理課程及時數詳如下表：

資訊安全認知教育訓練課程	對象	時數
資安月活動線上有獎徵答	全體員工	1,827 小時
資安講座 (烏俄戰爭中的虛擬砲火 - 現代資安作戰)	資安幹事、資訊安全組	100 小時
資安講座 (營業秘密案例分享)	單位主管、資訊安全組	104 小時
社交工程演練	全體員工 (不含 TA)	2,373 小時
社交工程教育訓練	演練點擊員工	198 小時
【全員閱讀】公司機密管理辦法	全體員工	1,489 小時
【全員閱讀】營業秘密案例分享與交流	全體員工	775 小時
合計		**6,866 小時**

為強化員工的資安意識，每年舉辦資安月活動，全體員工參與資安宣導短片製作，及相關執行成果詳如下：

項目	執行成果
提倡全體員工參與以小短片的方式呈現，透過周遭的現身說法及遭遇詐騙的經驗分享	投稿高達 35 個單位，每個單位投稿至少一份小短片
辦理兩場實體資安講座「烏俄戰爭中的虛擬砲火 - 現代資安作戰」、「營業秘密案例分享 (法務部調查局) 」	各單位主管及資安幹事參與人次超過 **120** 人次
全體員工參與資安政策及規定之題庫答題	全數答對比率 **99.9%**

資訊安全執行成果

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，2022 年執行成果詳如下表：

公司機密管理

執行措施

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。

執行成果

無機密洩漏事件。

社交工程演練

執行措施

每季進行 2 次社交工程偽裝寄送擬真釣魚郵件演練及設定演練目標，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。

執行成果

全年累計執行 8 次演練人次超過 2.8 萬人次。

資安防護與監控

執行措施

根據台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 情資，及本公司內部統計資料，自 110 年迄今，受到駭客嘗試入侵的事件不斷。為降低駭客入侵或資料外洩機會，避免外洩後遭受利用與威脅，本公司建置完整之網路縱深防禦系統、分析駭客入侵手法、持續修補系統漏洞、並建置專人監控機制。

執行成果

委由第三方進行滲透測試及紅隊演練作業。

營運持續

執行措施

1. 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。
2. 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。

執行成果

1. 2022 年需執行演練系統共有 17 個，達成率 100%。
2. 資訊系統未有發生服務中斷事件。

資安風險防護

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，2022 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