資訊安全

南亞科技為保護公司與客戶資訊的安全，積極推動資訊安全相關制度，已於2019年取得ISO 27001:2013資訊安全管理系統認證，首次驗證範圍DRAM技轉文件與自行研發之製程技術資訊，及其資訊流之資訊安全管理系統，包括相關之機房維運、網路服務、以及資訊系統之開發、操作、與維運，涵蓋廠區的DRAM研發、生產作業所用系統之資訊安全管理 (包含OA與網路系統、設計與光罩下線(Mask Tapeout)系統、EDA、產品測試服務及實驗室管理系統與生產製造PIS系統)及所有人員，以強化資安防護措施，確保公司順暢運作並取得供應商與客戶的信賴。

為更進一步的落實資訊安全管理，我們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。

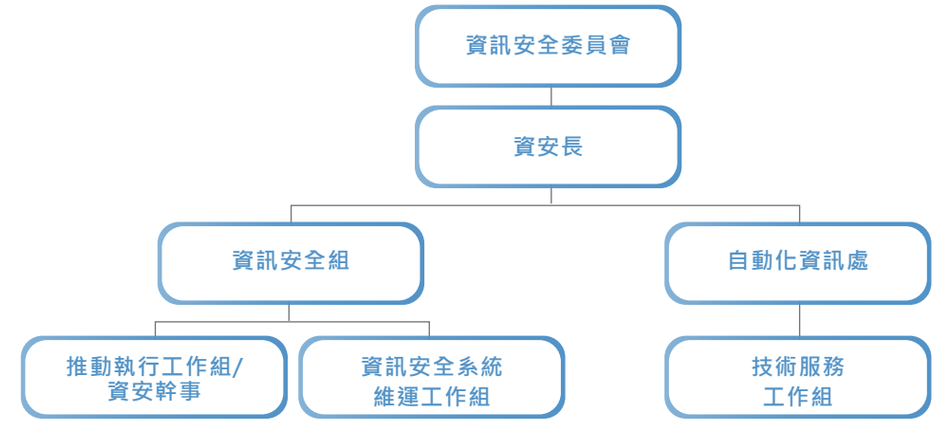
配合資通安全管理法實施，南亞科技比照資通安全責任等級A級之公務機關應辦事項，應持有4張有效資通安全專業證照，目前已取得EC-Council CCISO (Certified Chief Information Security Officer，資安長)、EC-Council ECSA (Certified Security Analyst，資安分析專家)、EC-Council CEH (Certificated Ethical Hacker駭客技術專家)及ISO/IEC 27001:2013 Information Security Management System(ISMS) Lead Auditor(ISMS主導稽核員)，提升公司資安人力專業職能以及執行效率。

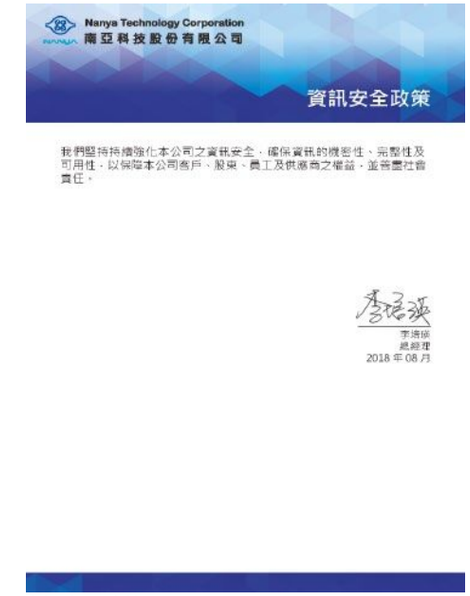
CCISO - 資安長證照

ECSA - 資安分析專家

CEH - 駭客技術專家

ISO 27001 Lead Auditor - 主導稽核員





資訊安全政策

ISO 27001證書

南亞科技資訊安全管理改善措施

本公司已取得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

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

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

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方案刻不容緩

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

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

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

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

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

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

資安風險評估與演練

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，每年執行復原演練，以確保系統正常運作。2021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畫表」定義之應變流程，通知應變單位執行因應措施。

資訊安全教育訓練與目標

在資安訓練部分，南亞科技投入許多資源，希望提升資安防護意識，針對全體員工，每年舉辦資安月活動，凝聚全員對資安防護的共識，每季亦進行社交工程演練；在資安的例行性會議中，資安月會會針對資安幹事進行宣導，資安季會中，則針對一級以上主管報告績效評比結果，而為了深植對機密資訊管理的文化，總部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，2021年完訓率為100%。

對象(部門及職類)	人數	人時數	涵蓋率
社交工程演練			
全體員工(不含TA)	27,583	2,299 小時	**100%**
社交工程教育訓練			
演練點擊員工	140	70 小時	**100%**
資安月活動-線上有獎徵答			
全體員工	3,423	1,712 小時	**99%**
常見社交工程攻擊手法解析與識別 (上)(下)			
全體員工	3,442	1,147 小時	**100%**
資安講座 - 從駭客視野，淺談開發與維運之間資安關係			
系統管理部、資訊安全組	43	43 小時	**100%**
資安講座 - 物聯網時代資安威脅管理新視野			
系統管理部、資訊安全組	58	87 小時	**100%**
資安講座 - 洞察並量化資產弱點以消弭資安風險			
系統管理部、資訊安全組	42	84 小時	**100%**
資安講座 - 一窺幾家駭客勒索集團技術手法-員工該有的資安認知及習慣			
資安幹事、資訊安全組、社交工程演練點擊員工	63	126 小時	**100%**
合計		**5,568小時**	

資訊安全目標

為落實資訊安全管理，並嚴格檢視執行狀況，我們針對資訊安全設定了量化管理目標，2021年針對機密性、完整性及可用性，共設定10項資安目標，除「電子郵件社交工程演練連結點擊及附件開啟率(%)」一項因採用擬真案例進行演練，部分同仁資安意識不足仍有點擊開啟狀況以致未達成目標外，其餘9項皆達成目標。

機密性	2021目標	年度平均	說明
資訊安全防護力指標	≥ 97%	99.1% (全年平均)	統計12個月未達標1次 (2021/03)
未經授權取得或使用技轉文件次數	每年0次	0	皆達標
AIP加密檔案於廠外未經授權開啟成功次數	每年0次	0	皆達標

完整性	2021目標	年度平均	說明
電子郵件社交工程演練連結點擊及附件開啟率 (%)	< 0.5%	1.0%	未達標，演練共8次 未達標3次(Q1、Q3、Q4)
OA Client Hot-Fix佈署完成率 (%)	≥ 99%	99.3%	皆達標
OA主動掃毒防護作業執行完成率 (%)	100%	100%	皆達標
(新增)發生駭客入侵重大資通安全事故	每年0次	0	皆達標(新增項目)

可用性		2021目標	年度平均	說明
OA System Down Time (Year)		< 1 min	0	皆達標
研發Database Down Time (Year)	設計	≤ 1次，< 24小時	0/0	皆達標
	技術開發	≤ 1次，< 24小時	0/0	皆達標

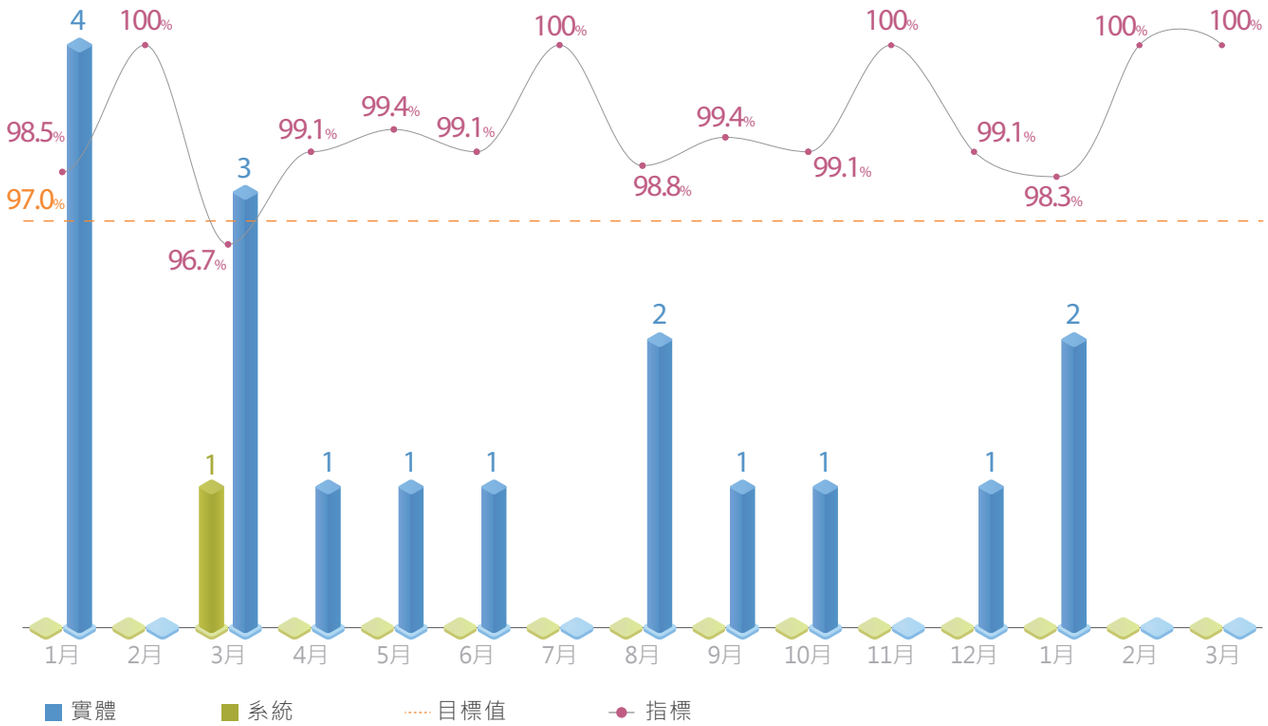
註： 針對績效未達標項目，於季會進行檢討改善報告，並開立e-CAR(矯正措施單)，遵循ISO 27001的PDCA改善循環

資安風險防護

我們了解資訊安全隨時面臨著風險，公司電腦全面佈署SEP(Symantec Endpoint Protection)防毒系統，搭配無塵室生產機台電腦MAC位址（Media Access Control Address）存取管控，防範電腦病毒攻擊。並使用Tenable的Nessus弱點掃瞄工具、找出線上系統、應用程式及電腦可能的重大漏洞與風險，提供系統管理人員掃瞄結果與病毒防治報告，做為系統必要的更新與升級之參考，並且即時更新屬高風險以上的系統漏洞，以增加系統安全性與穩定度。

為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方案刻不容緩，以AI技術分析搭配郵件附件清洗CDR (Content Disarm and Reconstruction)以降低社交工程風險，研析新興資安議題與資安攻擊手法，以預見資安威脅之發展與趨勢，同時洞悉未來資訊科技應用之資安風險，俾利及早提供防範作為。

資安防護力指標[註]



註：資訊安全防護力指標為每個月資安違規項目的統計指標，依據違規項目的風險與威脅，給與加權比重的計算，數值越高代表資安違規事件數越少或是資安威脅越低

資訊安全管理成效

	2018年	2019年	2020年	2021年
違反資安或網路安全事件 (件)	0	0	0	**0**
資料洩漏事件 (件)	0	0	0	**0**
涉及顧客個人資料之資安違反事件 (件)	0	0	0	**0**
因資料洩漏而受影響的顧客與員工人數 (人)	0	0	0	**0**
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	0	0	**0**