南緯實業股份有限公司
集團資訊安全管理辦法

本辦法於 110 年 11 月 11 日董事會同意

第一條　目的

為保護公司資訊資產，免於遭受破壞，不論這些破壞是來自於內部或外部人為、蓄意或意外，而制定集團資訊安全管理辦法，以作為實施各項資訊安全措施之標準。

第二條　適用範圍

有關資訊安全之事項，除另有規定外，悉依本辦法辦理。

第三條　名詞定義

無。

第四條　權責

資訊單位	處理資訊安全相關措施及技術規範的研議，以及資訊安全技之研究、建置及評估等相關事項，並會同稽核單位進行稽核作業。
人事單位	處理人員到職、離職的作業通知。
稽核單位	會同外部第三方相關單位辦理資訊機密維護及稽核等相關事項。
使用單位	依規範後的資訊工具與資訊系統操作等事項。

第五條　作業程序

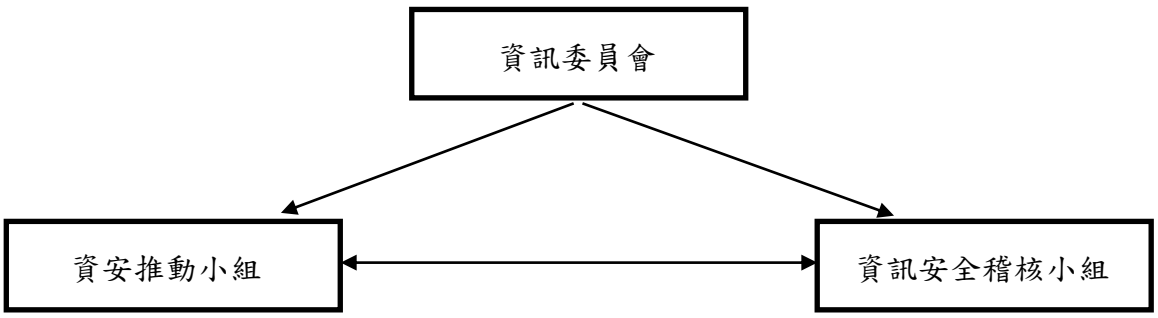
5.1　資訊安全政策評估

應由具專業技術及知識之資訊單位、內部稽核單位、人事單位及獨立客觀的主管人員辦理，並定期評估。

5.2　資訊安全組織與管理

為提升集團資訊安全管理與資訊安全相關政策執行與推動，由「資訊委員會」負責審視各子公司資安治理政策，並監督資安管理運作情形。

南緯實業股份有限公司
集團資訊安全管理辦法



資訊委員會	為任務編組方式組成，由管理部主管擔任召集人、各部級主管為委員，負責資訊政策制定及資訊管理事項之協調，如因職務調動即刻指派遞補人員與辦理交接。
資安推動小組	由資訊委員會執行幹事擔任組長並指派組員，負責規劃及執行各項資訊安全作業。
資訊安全稽核小組	由資訊委員會指派小組成員(含內部稽核人員)；負責評估與檢視資訊安全管理制度及執行情形。

5.3 資產管理

5.3.1 資訊資產應列冊管制，並隨時更新維護。

5.3.2 重要資訊資產應指定專人管理，並明定其責任。

5.3.3 安全等級要求高的資訊資產，應標示清楚，以利使用者遵循。

5.4 人力資源安全

5.4.1 新人報到或職務變動時，需填寫，【TR3-IT01-N 集團 ERP 帳號權限申請單】，經核決權限通過始可啟用。

5.4.2 新人報到及新業務需求產生，每一項資訊系統與設備的裝置及使用，需至 EIP 填寫【TR3-IT01-K 資訊服務需求申請單】依簽核流程申請後始得啟用。

5.4.3 員工使用資訊科技設備，應依相關內部規範及機密維護責任，於人事單位任用新進人員時，應簽署【TR3-HR01-F 網際網路暨電子郵件信箱使用規範書】，以明責任。

5.4.4 處理個人資料檔案人員，其職務如有異動，應將所保管之儲存媒

體及有關資料列冊移交,接辦人員應重置相關系統密碼及使用者帳號識別。

5.4.5　使用者密碼之管理

5.4.5.1 使用者密碼須為英文(大、小寫)+數字至少 6 碼之安全層級。

5.4.5.2 密碼需每季要求更換。

5.4.6　當人員任用及約聘僱條件或契約有所變更時，尤其是人員離職或是約聘僱用契約終止時，應重新檢討機密維護責任約之妥適性。

5.4.7　有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵件、電腦防毒等）之事項應隨時公告在 EIP 平台。

5.5 實體與環境安全

5.5.1　各資訊資產管理者應妥善地維護設備，以確保設備的完整性及可以持續使用。

5.5.2　儲存個人資料之電腦或設備如需報廢或轉移他用時，資訊單位應確實刪除該設備所儲存之個人資料檔案，並確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

5.5.3　資訊單位就系統伺服器主機設備安置於主機房，並由資訊單位專責管理，並管制非相關資訊、維修人員隨意進出，並於每次進出填寫【TR3-IT01-F 資訊機房進出管制紀錄表】。

5.6 通訊與作業管理

5.6.1　為確保系統安全控制不被破壞，應建立變更控制流程；任何的系統變更，皆應獲得權責管理人員的同意並至 EIP 填寫【TR3-IT01-I 集團系統維護申請單】，經核決權限通過。

5.6.2　所有連上網路的設備(Internet、Intranet)，或是由資訊服務提供者所維護的設備，需至 EIP 填寫【TR3-IT01-M 網際網路使用申請單】，依核決權限簽核並經由資訊單位的安全審查，始可上線使用。

5.6.3　軟體安裝須至 EIP 填寫【TR3-IT01-K 資訊服務需求申請單】進行申請，核准後由資訊人員協助安裝，並留下紀錄已備查詢。

5.6.4　內部所使用之授權軟體須建立紀錄，並填寫【TR3-IT01-H 資訊軟

體紀錄表】已備查詢。

5.6.5　網路安全管理：

5.6.5.1 應定期評估網路系統安全（例如：網路流量狀態、網路使用權限等），並留存相關紀錄。【TR3-IT01-B 資訊盤點維護檢核表】、【TR3-IT01-C 防火牆管控檢核表】

5.6.5.2 於雲端資安後台定期修補網路運作環境之安全漏洞（含伺服器、攜帶型、工作站端），並留存相關文件【TR3-IT01-B 資訊盤點維護檢核表】。

5.6.6　電腦病毒及惡意軟體之防範：

5.6.6.1 應採行必要的事前預防及保護措施，防制及偵測電腦病毒、特洛伊木馬及邏輯炸彈等惡意軟體的侵入，並填寫【TR3-IT01-D 日常維護紀錄表】以日後查考。

5.6.6.2 為使電腦病毒影響公司正常運作之程度降至最低，應建立妥適的業務永續運作計畫，將必要的資料及定期軟體備份，事前訂定回復作業計畫【TR3-IT01-G 還原演練紀錄表】。

5.7 存取控制

5.7.1　使用者本機或單位資料檔案應放在網路磁碟機公檔中，並依循「電腦檔案公檔管理辦法」歸列檔案。

5.7.2　公司敏感性資料如有需要被讀取或交流時，需至 EIP 填寫【TR3-IT01-L 公檔開放申請單】，經核決權限通過後始可開放。

5.7.3　於工作場所使用之公司資產的可攜式儲存媒體及設備(USB 裝置)，需要透過 EIP 行事曆借用已備紀錄，並註明設備使用用途。

5.7.4　非公司既有資產之可攜式設備，員工需至 EIP 填寫【TR3-IT01-K 資訊服務需求申請單】流程申請以記錄（管控範圍定義：筆記型電腦、USB 隨身碟、隨身硬碟)。

5.7.5　如有長期外借電腦設備需求時(例：外派、居家作業)，員工需至 EIP 填寫【TR3-IT01-K 資訊服務需求申請單】，經核決權限通過後於領取設備時填寫【TR3-IT01-J 資訊設備保管單】，以備查詢。

5.8 資訊系統取得、發展及維護

5.8.1 與公司往來資訊服務提供者，依「TR1-PL03 採購管理辦法」並由資訊單位評核委外服務合約與維持適當的互動管道，即時解決相關突發性的資訊安全問題。

5.8.2 外部連線(供應商)至內部主機進行更新或異常排除時，應填寫【TR3-IT01-A 外部廠商連線維護紀錄表】，留存主機系統更動紀錄。

5.9 資訊安全事故管理

5.9.1 應建立處理資安事件之作業流程，並給予相關人員必要的責任，以便迅速有效處理資安事件，緊急處理的各項行動，應詳細記載【TR3-IT01-E 資安事件紀錄表】，以備日後查考。

5.10 企業持續運作管理

5.10.1 為因應各種人為及天然災害造成業務運作受影響，資訊單位須定期進行資料備份。

5.10.2 發生資訊安全事件時，應立即向權責主管通報，由資訊單位聯繫檢警調單位偵查。

5.10.3 為保障企業營運秘密安全，資訊單位得對電子資料通訊做必要的監控與資料保存。

5.11 遵循事項

5.11.1 資訊作業遵行國際資安標準，並需符合國內外資訊安全法令規範。

5.11.2 禁止使用違反著作權、善良風俗或會妨害網路系統的正常運作之不法或不當的資訊。相關查核記錄應妥善保存。

第六條 使用表單

6.1 TR3-IT01-A 外部廠商連線維護紀錄表

6.2 TR3-IT01-B 資訊盤點維護檢核表

6.3 TR3-IT01-C 防火牆管控檢核表

6.4 TR3-IT01-D 日常維護紀錄表

6.5 TR3-IT01-E 資安事件紀錄表

6.6 TR3-IT01-F 資訊機房進出管制紀錄表

6.7 TR3-IT01-G 還原演練紀錄表

6.8 TR3-IT01-H 資訊軟體紀錄表

6.9 TR3-IT01-I 集團系統維護申請單(EIP)

6.10 TR3-IT01-J 資產設備保管單

6.11 TR3-IT01-K 資訊服務需求申請單(EIP)

6.12 TR3-IT01-L 公檔開放申請單(EIP)

6.13 TR3-IT01-M 網際網路使用申請單(EIP)

6.14 TR3-IT01-N 集團 ERP 帳號權限申請單(EIP)

6.15 TR3-HR01-F 網際網路暨電子郵件信箱使用規範書

第七條 參考文件

7.1 TR1-HR23 核決權限

7.2 TR1-PL03 採購管理辦法

7.3 電腦檔案公檔管理辦法