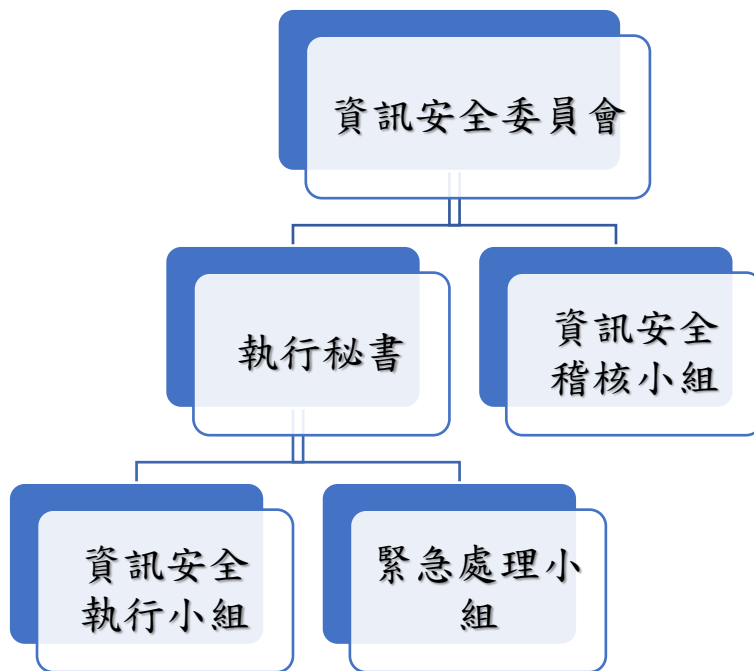


力山工業股份有限公司

資通安全管理及執行情形

資安政策的法源依據主要來自 ISO/IEC 27001 國際標準，作為技術與管理的核心框架。這些規範共同確保能系統化管理資訊安全風險，維護資訊資產的機密性、完整性與可用性。

組織架構:資訊安全委員會由資訊最高主管擔任召集人，各部門主管擔任成員，負責審查資訊安全管理相關事宜，視需要召開跨部門之資源協調會議，負責協調資訊安全管理制度執行所需之相關資源分配



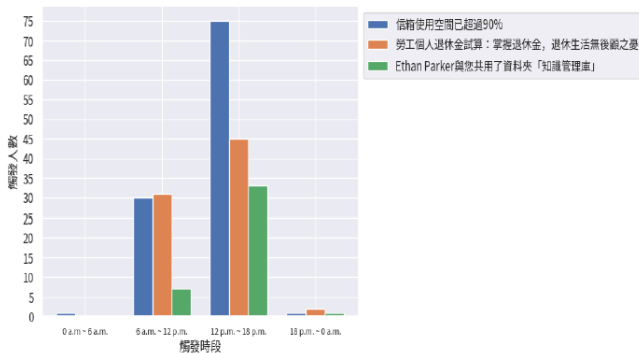
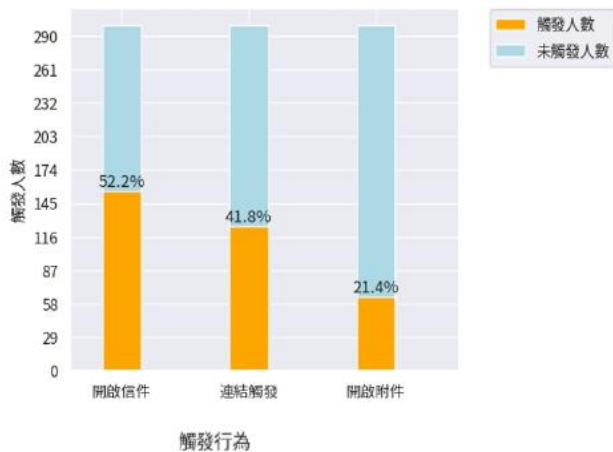
執行措施:

- 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
- 保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整；確保本公司關鍵核心系統維持一定水準的系統可用性。
- 每年進行查核並改善缺失，以確保資訊安全。

成果案例：

| 課程名稱 | 上課人數 | 合格人數 | 完成率 |
|-------------------------------|------|------|------|
| 網路釣魚防詐資安宣導 | 93 | 84 | 90% |
| 木馬攻擊 | 98 | 98 | 100% |
| 帳號被盜·個資外洩·加上假訊息攻擊！面對資訊戰你該怎麼做？ | 92 | 87 | 95% |
| Do Your Part Be Cyber Smart | 78 | 71 | 91% |
| APP 的誘惑 | 53 | 50 | 94% |
| 軟體更新為何很重要 | 80 | 77 | 96% |
| 使用 AI 工具需謹慎 | 106 | 95 | 90% |
| AI 工具的資安風險 | | | |
| AI 世代的資安危機 | 50 | 46 | 92% |
| 生成式 AI 的風險有哪些 | | | |

- 根據本公司修訂「網路及系統安全管理說明書」，內外部人員連線皆需要填寫相關申請後才得以存取。每年關鍵核心系統皆有簽訂維護合約，確保維持系統可用性。
- 於 2025 年 7 月進行兩大關鍵核心系統的備份還原演練，2025 年 8 月執行社交工程演練，並請觸發釣魚信件的同儕進行教育訓練。

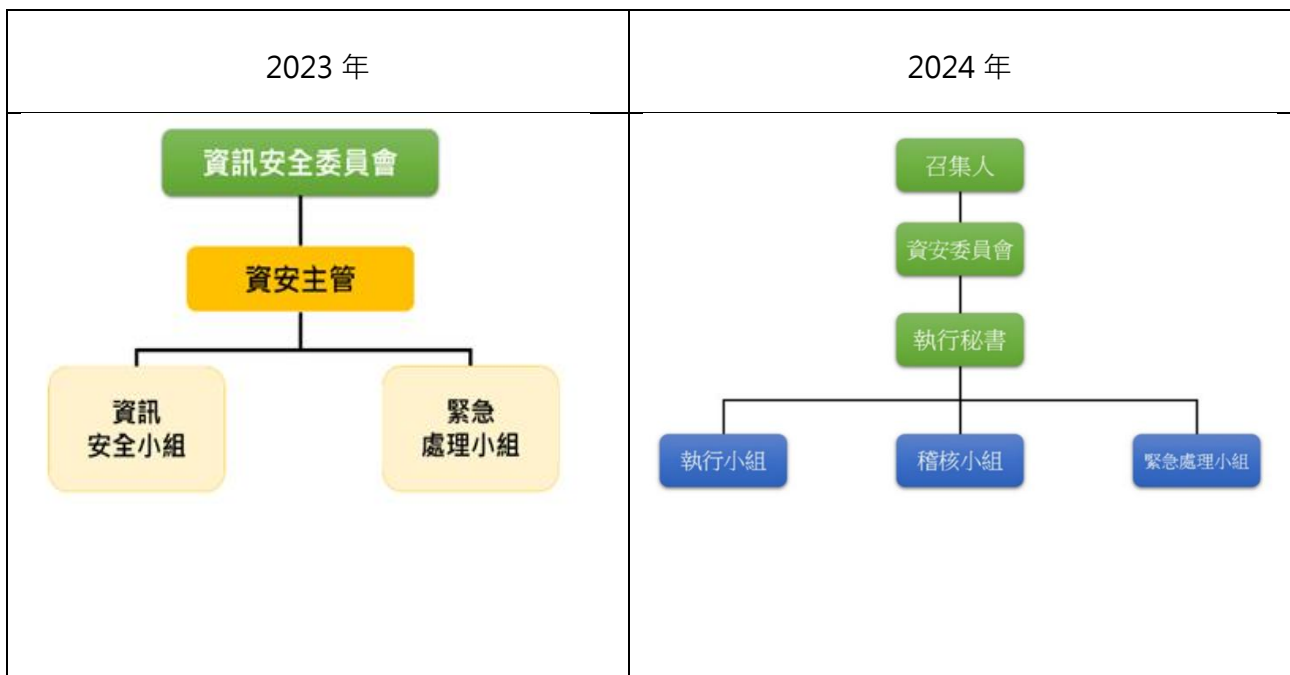


- 2025 年完成一次 ERP 及 PLM 系統的還原演練，以確保營運持續運作。
- 根據「資訊安全目標有效性量測表」非預期中斷時間單次超過 8 小時的件數為 0 件
- 每年根據矯正處理單做缺失改善，並且定期追蹤改善成效，以降低公司資訊安全風險。

因應企業永續發展 (ESG) 之需要以及配合國際資安技術與國內外法規等要求，力山於 2024 年 10 月取得「ISO27001:2022 資訊安全管系統驗證」，期間擴大「資訊安全委員會」組織，以提升組織資訊應對能力與降低資安風險，由專人專責資訊安全保護政策的制定、執行、風險管理並進行合規性稽核要求。

本公司資安業務由資訊部負責，為健全資訊安全符合上市上櫃公司資通安全管控制引規定，依 2023 年底依金管會「公開發行公司建立內部控制制度處理準則」設置資安專責主管及至少 1 名資訊安全專責人員。

本公司資安業務由資訊部負責，為健全資訓安全並符合法令規定，原 2023 年底依金管會「公開發行公司建立內部控制制度處理準則」設置資安專責主管及至少 1 名資訊安全專責人員。配合 ISO27001 導入等組織規範，於 2024 年調整資安委員會架構除新增稽核小組 4 人外並增加組織召集人 1 名及執行秘書 1 名，以提高資訊安全內稽內控之風險管理能力。



資訊安全管理

力山依 ISO 27001 CIA 三原則：機密性(Confidentiality)、完整性(Integrity) 及可用性(Availability) 目標，制定資訊安全政策作為最高指導原則，並導入資訊安全管理系統，以週期性規劃、執行、查核

及改進的流程模式，確保資訊業務運作的效能與持續性。



在本公司，資訊安全管理體系（ISMS）的實施是基於國際標準 ISO27001，並通過 PDCA（Plan-Do-Check-Act）循環來持續改進和增強。我們承諾保護資訊資產並確保資訊安全，這是我們整體 ESG（環境、社會與治理）策略中的關鍵組成部分。

計畫（Plan）： 我們制定了詳細的資訊安全政策與目標，並通過風險評估和風險處理計劃來識別和分析現有的資訊安全風險。資源配置、控制措施的設計和實施是我們首要的工作，確保資訊安全管理體系能夠有效運行。

執行（Do）： 在執行階段，我們根據既定的計劃，實施各種資訊安全管理措施，包括員工培訓、技術控制措施的部署以及文件和記錄的建立和維護。我們重視培養員工的資訊安全意識，並確保他們具備必要的知識和技能來保護公司資訊。

檢查（Check）： 我們定期監控和評估資訊安全管理體系的運行情況，並進行內部審核，確保資訊安全措施的有效性和合規性。此外，我們分析安全事件和事故，識別改進的機會，不斷優化管理體系。

行動（Act）： 根據檢查階段的結果，我們採取適當的改進措施，包括策略調整、控制措施改進、加強培訓或修訂政策和程序。我們致力於持續改進，確保公司能夠應對不斷變化的風險和挑戰。

通過不斷重複這個 PDCA 循環，組織可以持續改進其資訊安全管理體系，應對不斷變化的風險和挑戰。

具體作為

公司每月進行資安宣導及臨時應變會議，針對新近內外部資安議題進行討論及對策研擬，並落實於年度計畫中。年度活動涵蓋資安政策及程序書的評估修訂、重大及高風險主機弱點的處理、定期資訊安全與個資宣導教育訓練，以及每年定期社交工程郵件演練。此外，公司每年安排第三方外部稽核及一次內部稽核審查，確保資訊安全管理系統的實施成效及各項目標的達成。在建置多層次資訊安全管理

的同時，力山還利用如 TWCERT/CC 等聯防機構提供的威脅情報進行風險評估與處理，以預防及降低潛在風險。

自 2024 年 10 月取得「ISO 27001 資訊安全管理系統驗證」起，力山將以每年通過評鑑為目標，持續精進資訊安全能力來保障公司人員、數據、資訊系統、設備及網路的安全。

| 年度 ISO27001 管理要點 | | | |
|------------------|----------------------------------|------------------------|---|
| 管理要點 | 執行單位 | 執行次數 | 說明事項 |
| 資訊安全委員會 | 召集人、資安委員會、執行秘書、執行小組、稽核小組、緊急處理小組。 | 每年一次管理審查會議 | 負責制定策略、管理風險、配置資源、監督評估和應急處理，以提升公司的資訊安全管理水準。 |
| 資安政策 ISMS 程序書 | 執行小組、稽核小組、緊急處理小組。 | 每年評估審閱一次 | 確保資訊安全管理體系的標準化和一致性，並為組織提供明確的指導和操作流程以管理資訊風險。 |
| 資安會議 | 召集人、執行小組、稽核小組、緊急處理小組。 | 每月進行資安宣導 每年一次管理審查會議 | 1. 資訊安全管理相關議題進行討論及追蹤，確保策略及措施的落實 2. 資安系統運作的整體效能進行全面性檢討，確保持續改進與符合國際標準 |
| 資核活動 | 召集人、執行小組、稽核小組、緊急處理小組。 | 每年一次內部稽核 每年一次外部稽核 | 1. 為確保資訊安全管理系統的合規性與有效性，公司每年進行一次內部稽核，透過自我審查發掘改進空間 2. 第三方專業機構檢視系統運行狀況，以確認其符合 ISO 27001 的要求 |
| 資安宣導 | 執行小組 | 每月資安海報宣導 | 透過資安海報進行宣導，強化全體員工的資安意識，讓資訊安全成為公司文化的重要一環 |
| 教育訓練 | 執行小組 | 力山學院進行線上學習資安課程 | 為提升員工的資訊安全專業知識與技能，透過「力山學院」提供線上學習平台，安排多樣化的資安課程，確保全體員工具備應對資訊安全挑戰的能力 |
| BPC | 緊急處理小組 | 每年一次營運持續演練 | 營運持續計畫(BCP)演練係為確保災難事件發生後，BCP 相關應變計畫可立即啟動並確實可行，以使關鍵營運項目在復原目標時間內恢復至正常狀態。 |
| DRP | 緊急處理小組 | 每年一次災害還原演練 | DRP 災難復原演練是一種測試和模擬災難發生後，企業或組織如何應對和復原的練習。 |
| 社交工程演練 | 執行小組 | 每年進行一次社交工程演練 | 模擬可能的外部攻擊場景，測試員工對資安威脅的應對能力，並透過結果分析持續優化防護措施。 |
| 主機弱點掃描 | 執行小組 | 每年一次的弱點初掃與複掃作業 | 包括初掃與複掃，檢測潛在安全風險，並即時修復弱點，以降低資訊系統受到攻擊的可能性，確保系統安全 |

2024 年依據 ISO27001 進行風險評鑑辦法建立風險評估準則，針對資產盤點七大類依人員、文件、軟體、通訊、硬體、資料、環境分類，並依資訊資產價值 C.I.A 原則與威脅弱點評估找出資安風險較高之項目共 17 項。經資訊安全委員會討論決議全面升級 ERP 與 PLM 等兩大核心系統，列入 2024 年改善事項，共投入 NT\$4,327,449 將於 2025 年完成升級，確保更完善的資安系統環境，降低系統資安攻擊而導致公司正常營運之潛在風險。

資通安全政策

壹、目的

力山工業股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

貳、適用範圍

本公司所有單位。

參、定義

無。

肆、願景與目標

一、資訊安全政策願景：

- 1.強化人員認知、避免資料外洩。
- 2.落實日常維運、確保服務可用。

二、依據資訊安全政策願景，擬定資訊安全目標如下：

- 1.辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
- 2.保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
- 3.定期進行稽核作業，確保相關作業皆能確實落實。
- 4.確保本公司關鍵核心系統維持一定水準的系統可用性。

三、應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本公司「監督與量測管理程序書」辦理。

四、資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。

伍、責任

- 一、本公司的管理階層建立及審查此政策。
- 二、資訊安全執行小組透過標準和程序以實施此政策。
- 三、所有人員和委外服務供應商均須依照相關安全管理程序以維護資訊安全政策。
- 四、所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
- 五、任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

陸、審查

一、本政策應至少每年審查 1 次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及資訊安全實務作業能力。

柒、實施

- 一、任何機關單位因業務需求取得本公司機敏性資訊或個人資料時，應負起資料保密責任及妥善運用，並遵守國家相關之法令及本公司之相關資訊安全規定。
- 二、若因機關單位疏失造成資料外洩或資安事件，應負相關法律責任。

三、各單位執行資訊安全管理作業，如下列項目需進行變更，應依規劃之方式執行變更：

- 1.資訊安全管理系統變更。
- 2.發生重大資安事故。
- 3.有新增、變更或移除資訊資產。
- 4.作業環境改變。

四、如需進行資訊安全管理系統變更，應考量下列事項：

- 1.變更的目的與其潛在之影響。
- 2.管理系統的完整性。
- 3.資源的可用性。
- 4.職責與權限之分配或重新分配。

捌、附則

- 一、本規定於呈總經理核准後實施，修改時亦同。