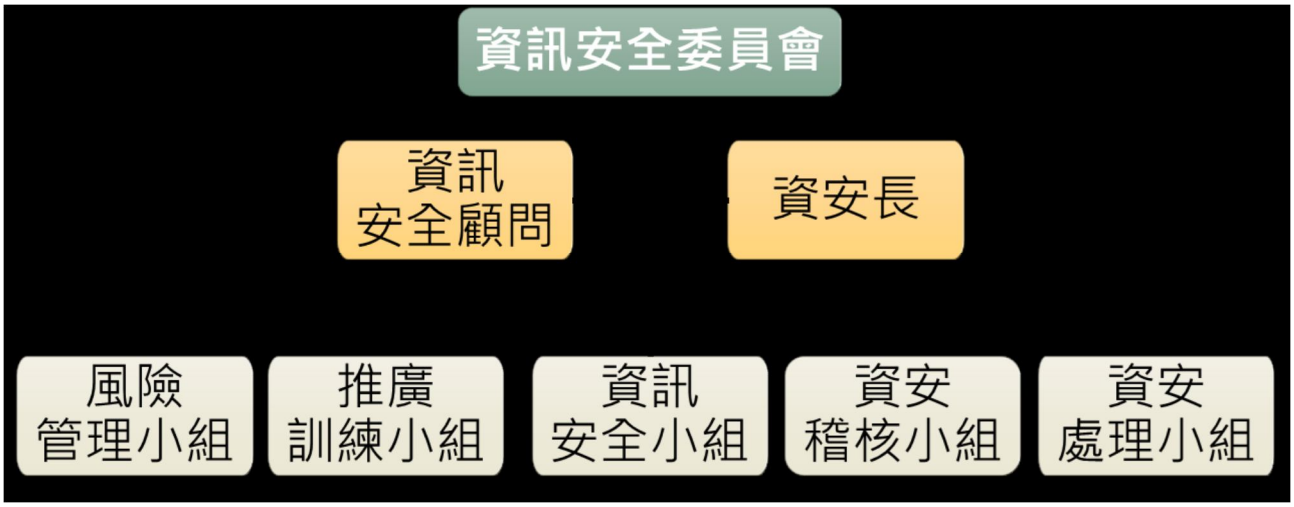
力山工業股份有限公司

資通安全管理

(一). 敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

1. 資訊安全風險管理架構；本公司強化資訊安全管理，確保資訊資產之機密性、完整性及可用性，以提供本公司之業務持續運作之資訊環境。本公司雖尚未成立跨部門資訊安全委員會，目前由資訊管理部上層總管理處主管兼任。
2. 資通安全政策
   (1). 目前由總管理處下資訊管理部負責，統籌所有資訊安全管理相關事宜。
   (2). 訂定定期盤點資訊資產及個人資料清冊，依資訊安全及個人資料風險評鑑進行風險管理，落實各項管控措施。
   (3). 不定期辦理資訊安全及個人資料報護教育訓練及宣導作業，新進人員須簽署資通安全保密協定。
   (4). 本公司人員應遵守公司資訊或保密安全規範。
   (5). 本公司供應商及委外廠商應遵守本公司資訊安全規範約定。
   (6). 重要資訊系統或設備已建置適當備份及備援。
   (7). 要求個人電腦均安裝防毒軟體並定期更新，並禁止使用未經授權的軟體。
   (8). 建立業務持續運作管理機制，並每年定期實施內部稽核以確保資訊安全及個資保護管理制度之有效性。
3. 資安具體管理方案及投入資通安全管理之資源：
   (1). 資訊資產安全管理。
   (2). 網路及電腦系統安全管理。
   (3). 系統存取控制、發展及維護安全管理。
   (4). 外包專業電腦資訊廠商之維護服務。
   (5). 將資訊安全及個資保護檢查控制作業，列為年度稽核項目。
   (6). 每年度內部控制制度自行檢查作業，將實施成效提報董事會，並出具內部控制制度聲明書。

資訊安全專責



資訊安全管理與資料保護

公司依 ISO 27001 CIA 三原則：機密性(Confidentiality)、完整性(Integrity)及可用性(Avaliability)制定相關策略或評估潛在的威脅與漏洞並透過安全管制措施，保護資訊資產免於受到危害，以達到 CIA 之管理目標；對於資料控管制度依三原則中的機密性(Confidentiality)，來限制未經授權的資料之訪問與修改權，以確保侵犯客戶隱私並防止客戶資料遺失，進而支持組織的業務流程，以創造價值與實現組織的使命與願景。

資安防護

為因應未來流量的需求及提升資安的防護，公司建置多層防禦能力，對外：購置 NGFU palo alto 防火牆防止已知漏洞入侵、惡意軟體、間諜軟體和惡意 URL，同時針對未知的惡意軟體進行流量分析並自動提供保護，對內：增加第二台 NGFU 與 EDR 端點防護能力，面對新型態的加密攻擊做即時有效的攔阻防止擴散。

異地備援

公司為完善本地及異地備份備援架構機制，建構異地雲端機房(IDC)，機房符合 Tier III 認證等級最高規格，並同時在資安方面獲得 ISO27001 及 CSA STAR 最高階認證，另外也取得服務保證及客戶滿意度

的 ISO20000 認證等，除了可優化儲存效能及提升儲存空間使用量、簡單、全面的備份和歸檔外，並達到災害復原與業務營運不中斷的目標且適應未來的彈性擴充需求及符合資安法規要求。

員工資安訓練(本項教育訓練時數參考資通安全法)

依據資通安全管理法，針對在職人員透過定期的資安教育訓練海報/影片宣導強化員工的資安意識，資通安全專職(責)人員，每人每年需進行 12 小時課程練或資通安全，一般使用者每人每年 3 小時之資通安全教育訓練。

資訊風險管控

為達成公司可長可久的資安治理方式，在資安風險管控的整體業務活動與其所面臨的風險之下建立、實施、運作、監控、審查，並且維持和改進一個已經有文件化的管理制度，運用 PDCA（Plan-Do-Check-Act）過程導向模式，作為整體管理制度運作的基礎，來確保公司資安永續。