山隆通運股份有限公司

Shan-Loong Transportation Co., Ltd.

文件名稱：對子公司資訊單位之監督管理辦法
文件編號：CP052
權責部門：資訊處
發行日期：2026 年 01 月 27 日

文件修訂要點			
版次	生效日期	制修訂單位	修訂內容
A0	2026.01.27	資訊處	新制訂

1. 目的：本辦法旨在透過「授權管理、協同一致、嚴密監控」之機制，確保子公司資訊發展策略與集團整體目標一致，建立標準化且一致之資訊安全防護體系，並藉由定期回報與稽核機制落實風險控管，以維護集團商譽並有效降低法規遵循成本。
2. 範圍：本辦法適用於本公司直接或間接持股超過 50%，或具有實質控制權之國內外子公司（以下簡稱「子公司」)。
3. 權責：
   3.1. 制訂單位：本辦法之制訂及修正單位為資訊處。
   3.2. 適用單位(人員)：本辦法適用於本公司直接或間接持股超過 50%，或具有實質控制權之國內外子公司。
4. 名詞定義：
   4.1. 子公司：指本公司直接或間接持股超過 50%，或具實質控制權之公司。
5. 內容說明：
   5.1. 建立統一的資訊治理框架
      5.1.1. 政策一致性：子公司應參照本公司之資安政策（Information Security Policy)，制定所屬之資訊作業規範，且其安全性不得低於本公司標準。
      5.1.2. 職責劃分(SoD)：子公司資訊單位應設立明確職位說明書。涉及系統開發、維運、資安監控之職能應適度分離，以防範未經授權之異動。
      5.1.3. 重大決議報備：子公司針對重大資訊設備採購、關鍵系統更換，應事先報請本公司資訊單位審核。
   5.2. 資訊系統與基礎設施
      5.2.1. 獨立與介面安全：子公司應建立獨立營運之資訊系統，若需與本公司系統對接（如 ERP 合併報表、電子公文)，必須通過本公司之安全性檢測，並採取加密傳輸及防火牆隔離。
      5.2.2. 軟硬體規範：子公司之基礎設施（如伺服器品牌、端點防護軟體、作業系統版本）應符合本公司規定之技術藍圖，以利集團資源整合與弱點管理。
      5.2.3. 雲端服務管理：子公司導入雲端服務（SaaS/PaaS/IaaS）前，應進行供應商風險評估，並報備本公司備查；涉及機敏資料或核心業務之雲端服務導入，需經本公司資訊單位核准後始得進行。
   5.3. 資訊收集與報告
      5.3.1. 子公司應建立常態化之資訊收集與回報機制，定期向本公司資訊單位提報。
      5.3.2. 子公司提報之定期月報內容須包含系統可用率、機房維運狀況、資安演練結果及人員異動資訊。
      5.3.3. 子公司提報之關鍵績效指標（KPI）須包含系統可用性（目標達 99.9% 以上)、高風險漏洞修補率（原則上於公告後 14 日內完成，未能修補者須提出補償性控制措施並經核准)，以及資安事件之類型、次數與處理時程統計。
   5.4. 重大事件通報與應變
      5.4.1. 子公司發生重大資安威脅（如勒索軟體攻擊或資料外洩)、系統中斷致業務停擺超過

四小時，或涉及司法機關調查及重大法規違規事件時，資訊主管應於二小時內以即時通訊軟體或電話方式通報本公司，並留存相關紀錄，另應於二十四小時內完成並送達書面報告。

5.5. 法令遵循

5.5.1. 子公司之資訊作業應嚴格遵守營運所在地之法律（如台灣《個人資料保護法》；歐盟 GDPR 等）。涉及跨境數據傳輸時，應先行諮詢本公司法務與資訊單位。

5.6. 風險評估與營運持續

5.6.1. 風險評估：子公司應每年進行一次資訊安全風險評估，識別關鍵資產與威脅，並制定風險處置計畫。

5.6.2. 災害復原演練：子公司每年應針對核心業務系統進行至少一次災難還原演練，並將演練報告提交本公司。

5.7. 風險管理與稽核

5.7.1. 定期稽查：本公司資訊單位得每年至少一次，會同內部稽核單位對子公司進行現場或遠端稽查。

5.7.2. 專案稽核：針對發生重大資安事件或績效嚴重缺失之子公司，本公司得進行專案稽核，要求其限期改善。

5.7.3. 第三方稽核：必要時，本公司可委託第三方外部專業機構對子公司進行滲透測試或 ISO 27001 合規性檢查。

5.7.4. 稽核缺失未於限期內改善者，將列入子公司年度績效考核扣分項目，嚴重者議處相關人員。

5.8. 導入與實施程序

5.8.1. 現況診斷：實施初期，本公司應對各子公司進行資訊能力評級（Baseline Assessment）。

5.8.2. 溝通共識：定期召開集團資訊單位主管聯席會議，滾動式修正管理指標

5.8.3. 滾動修正：本辦法應配合技術趨勢（如 AI 治理、零信任架構）進行每年度之條文檢討。

6. 控制重點：

6.1. 本辦法依照相關法令之指引內容訂定管理計畫並據以執行。

6.2. 確保子公司資訊政策與本公司一致，避免治理落差風險。

6.3. 建立即時通報與定期回報機制，防止重大事件延誤處置。

7. 附件：無

8. 實施與執行：

8.1. 本辦法經董事會核定後實施；修正時，亦同。