



---

# 巨路國際股份有限公司

## 資訊安全政策

編號：LMX-Z-01

版次：1.6

---

發布日期：2025 年 09 月 01 日

---

編 號	LMX-Z-01	資 訊 安 全 政 策	等 級	一般
版 次	1.6		版 本 日 期	2025/09/01

文件制/修訂紀錄					
版 次	發 布 日 期	制/修訂說明	維 護 單 位	編 撰 者	核 准 者
1.0	2018/12/04	初次制定	資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.1	2020/09/21		資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.2	2022/06/27		資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.3	2023/09/27		資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.4	2023/11/01		資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.5	2024/02/21		資安合規 小組	陳俐蘋 (Apple_Chen)	資安長
1.6	2025/09/01	配合推動 ISO/CNS 27001 修訂	資安合規 小組	陳俐蘋 (Apple_Chen)	資安長

編 號	LMX-Z-01	資 訊 安 全 政 策	等 級	一 般
版 次	1.6		版 本 日 期	2025/09/01

目 錄

一、 目的.....4

二、 依據.....4

三、 目標.....4

四、 適用範圍.....4

五、 原則.....4

六、 實施方式.....5

編 號	LMX-Z-01	資 訊 安 全 政 策	等 級	一般
版 次	1.6		版 本 日 期	2025/09/01

## 一、目的

為強化資訊安全管理，確保資料、系統、設備及網路安全，有效降低因人為因素、天然災害等導致之資訊資產毀損、洩漏等風險，特訂定本政策以達成公司系統資訊之機密性、完整性及可用性之保全。

## 二、依據

參照下列相關法令及制度訂定本政策：

- (一) ISO/IEC 27001:2022
- (二) 個人資料保護法
- (三) 營業秘密法
- (四) 公司電腦化資訊系統處理循環內部控制制度暨相關管理辦法
- (五) 上市上櫃公司資通安全管控指引

## 三、目標

本公司資訊安全目標為：確保重要資訊及服務之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）與遵循性（Compliance）。並依各階層與職能定義及量測資訊安全績效之量化指標，以確認 ISMS 實施狀況及是否達成資訊安全目標。

## 四、適用範圍

- (一) 所有與本公司適用範圍內之內部人員、服務供應商及訪客等，應遵循本政策及 ISMS 各項程序。
- (二) 公司整體資訊環境、公司各項資訊資產。

## 五、原則

- (一) 各項資訊安全規定必須遵守法規及配合公司實際營運作業。
- (二) 資訊安全制度之建立及推動事宜。
- (三) 定期執行資訊系統之資產及風險評鑑，以依據進行對應之安全規劃。
- (四) 建立資訊硬體設施及軟體之管理機制，以統籌分配、有效運用資源。
- (五) 明確規範資訊系統及網路服務之使用權限，防止未經授權之存取行為。
- (六) 電腦機房實體及環境安全防護措施，並定期施以相關檢驗。
- (七) 明訂系統與網路之操作管理，以維持資訊系統與網路環境之正常運作。
- (八) 資訊系統於建置及維護時將資訊安全因素納入，防範危害系統安全之情況。
- (九) 設立資訊安全事件發生之處理程序，降低災害之影響。
- (十) 訂定資訊安全之營運持續計畫並實際演練，確保公司資訊業務正常運作。

編 號	LMX-Z-01	資 訊 安 全 政 策	等 級	一般
版 次	1.6		版 本 日 期	2025/09/01

- (十一) 制定系統文件管理程序，以保持文件紀錄之機密性及完整性。
- (十二) 定期資訊安全稽核作業，定期檢視資訊安全制度落實情形。
- (十三) 資訊安全政策應定期進行評估，以反映資訊安全管理、法令、技術及公司營運之最新狀況，並確保資訊安全實務作業之可行性及有效性。
- (十四) 若因相關法令及制度之版本修訂，需進行資訊安全管理系統之變更，應以專案方式進行評估規劃及盤點，並公告資訊安全委員會進行各事項之審核追蹤。

## 六、實施方式

- (一) 將資訊安全整合於各項資訊專案管理作業中，包含風險評鑑、資訊安全要求事項、風險處理追蹤及控制機制之稽核。
- (二) 推動公司資訊安全訓練，以充份了解本政策及相關規範及保護公司資訊資產安全之責。
- (三) 公司人員應配合資訊安全政策及相關控管措施，若違反相關執行法則造成公司損失者，應依據「MP0101 工作規則」之懲處條例辦理處置；另因違規造成的費用(例如需補足合法軟體授權之費用)也應由違法人員全額負擔。
- (四) 由資訊安全委員會每年定期對本政策之作業進行審議，組織、業務、法令或實體環境等因素之變遷時，予以適當修訂。
- (五) 本公司 ISMS 文件(包含本政策)制定或修訂後，應以網站公告、電子郵件、通訊軟體、文件管理系統、會議或其他可溝通或傳達方式，告知或與內外部關注方溝通，如：內部員工、客戶、合作夥伴、供應商等。
- (六) 由經管會對本政策及相關規範進行督導執行之職責。
- (七) 本政策經董事長核定公布施行，修正時亦同。