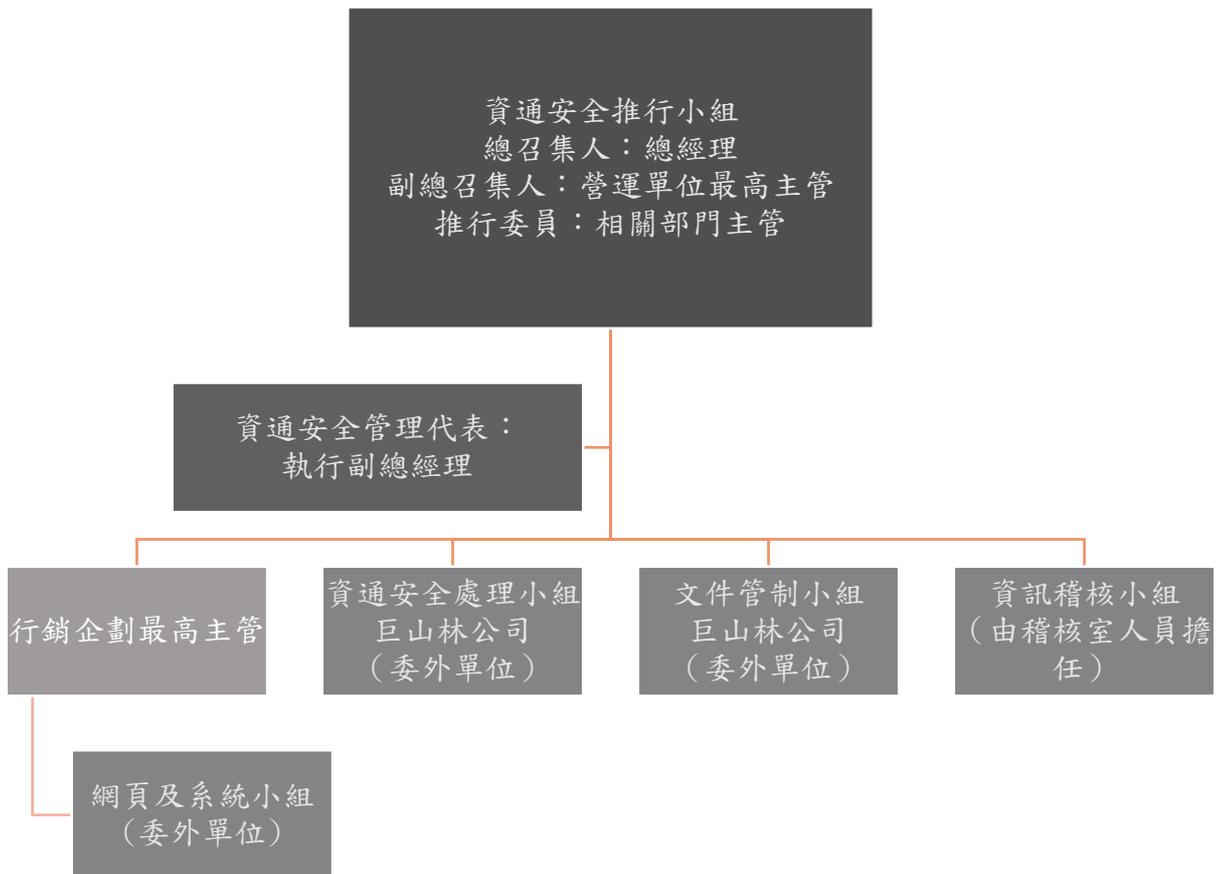


# 力麗觀光開發股份有限公司

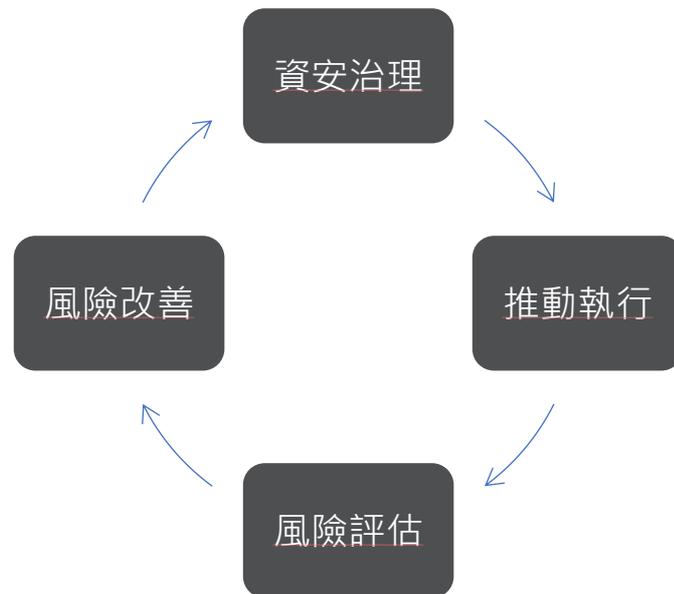
## 資訊安全政策及管理方案

### 一、 資訊安全風險管理架構



- 本公司資訊安全之權責單位為資通安全推行小組，該單位由資通安全管理代表、總召集人、營運單位最高主管、相關部門主管及資訊稽核組成，上述小組協同資通安全委外單位，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實。
- 本公司稽核室為資訊安全稽核單位，該室設置專職稽核人員，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。

- 組織運作模式-採 PDCA ( Plan-Do-Check-Act ) 循環式管理，確保可靠度目標之達成且持續改善。



## 二、 資訊安全政策

本公司資訊安全管理機制，包含以下四個面向：

- (一) 制度規範：訂定公司資訊安全管理制度，以規範人員作業行為。
- (二) 科技運用：建置資訊安全管理設備，落實資安管理措施。
- (三) 人員宣導：進行資訊安全宣導，提昇全體同仁資安意識。
- (四) 供應商管理：明定廠商之資訊安全責任與保密規定，要求依安全管理程序確保資訊安全。

管理措施說明如下：

- 制度規範：本公司內部訂定資安規範、制度以及人員資訊安全規範，每年定期檢視上述制度是否符合營運環境變遷，並依需求適時調整。
- 科技運用：本公司為防範各類外部資安威脅，建置必要之資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。
- 人員宣導：本公司定期實施人員資訊安全教育宣導，藉以提昇內部人員資安意識。

- 供應商管理：事前研提資訊安全需求，明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期予以查核。委外服務廠商均須依照相關安全管理程序以確保資訊安全。

### 三、資訊安全具體管理方案

本公司實施之資訊安全具體管理方案如下：

資訊安全管理措施		
類型	說明	相關作業
權限管理	人員帳號、權限管理、系統操作管理措施	<ul style="list-style-type: none"> <li>●人員權限管理與審核</li> <li>●人員帳號權限定期盤點</li> </ul>
存取控制	人員存取內外部系統、操作行為軌跡管控	<ul style="list-style-type: none"> <li>●內/外部存取管控措施</li> <li>●操作行為軌跡管控措施</li> </ul>
外部威脅	內部系統潛在弱點、病毒防護措施	<ul style="list-style-type: none"> <li>●主機/電腦弱點偵測及更新措施</li> <li>●病毒防護與惡意程式偵測</li> </ul>
系統可用性	系統可用狀態、服務中斷處置措施	<ul style="list-style-type: none"> <li>●系統/網路可用狀態監控及通報機制</li> <li>●服務中斷之應變措施</li> <li>●資料備份措施、本/異地備份機制</li> <li>●定期災害還原演練</li> </ul>
資安通報應變	資安通報處理程序	<ul style="list-style-type: none"> <li>●加入 TWCERT 資安情資分享組織</li> <li>●訂定資安事件應變處置及通報程序</li> </ul>

### 四、實施：

本資訊安全政策及管理方案經董事會通過後實施，修正時授權董事長決議。

制定日期：110 年 8 月 11 日。

第一次修訂：111 年 11 月 21 日。

## 投入資通安全管理之資源

資通安全推行小組依據五大類資訊安全具體管理方案，投入之資源如下：

- (一) 網路硬體設備：防火牆、郵件防毒、垃圾郵件過濾、負載平衡器等。
- (二) 軟體系統：端點防護系統、備份管理軟體、VPN 認證等。
- (三) 投入人力：每日系統狀態檢查、每週定期備份及備份媒體異地存放之執行、不定期執行資安宣導、每年對資訊循環之內部稽核、會計師稽核等。
- (四) 資安通報應變：加入 TWCERT 資安情資分享組織，並訂定資安事件應變處置與通報程序。