

**力麗觀光開發股份有限公司**  
**資通安全風險管理執行情形報告**

執行年度	112 年度	董事會 報告日期	112 年 12 月 11 日																				
執行單位	總經理室	報告人	楊崢如總經理																				
說明	為維護本公司資訊安全，定訂相關規章，達公司資訊之安全防護。																						
執行情形	<p>一、本公司已訂定「資訊安全政策及管理方案」並於公司網站公告。</p> <p>二、資通安全推行小組於 112 年依「資訊安全政策及管理方案」之資訊安全政策執行，隨時更新相關法令訊息，適時檢視資通安全政策之有效性。</p> <p>三、112 年度資通安全推行小組實施之資訊安全具體管理方案如下，第 2 次修正之「資訊安全政策及管理方案」依辦法規定，於同年 11 月經董事長核准修訂。</p>																						
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3" style="background-color: #333; color: white; text-align: center;">資訊安全管理措施</th> </tr> <tr> <th style="width: 15%;">類型</th> <th style="width: 55%;">說明</th> <th style="width: 30%;">相關作業</th> </tr> </thead> <tbody> <tr> <td>權限管理</td> <td>人員帳號、權限管理、系統操作管理措施</td> <td> <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> </td> </tr> <tr> <td>存取控制</td> <td>人員存取內外部系統、操作行為軌跡管控</td> <td> <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> </td> </tr> <tr> <td>外部威脅</td> <td>內部系統潛在弱點、病毒防護措施</td> <td> <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> </td> </tr> <tr> <td>系統可用性</td> <td>系統可用狀態、服務中斷處置措施</td> <td> <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> </td> </tr> <tr> <td>資安通報應變</td> <td>資安通報處理程序</td> <td> <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> </td> </tr> </tbody> </table>			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
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>																					
	<p>四、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：</p> <p>(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。</p> <p>(二) 軟體系統：端點防護系統、備份管理軟體、VPN 認證等。</p> <p>(三) 投入人力：</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 10px 0;"> <tr> <td style="width: 20%;">每日</td> <td>系統狀態檢查</td> </tr> <tr> <td>每周</td> <td>定期備份及備份媒體異地存放之執行</td> </tr> <tr> <td>不定期</td> <td>執行資安宣導</td> </tr> <tr> <td>每年</td> <td>資訊循環之內部稽核、會計師稽核</td> </tr> </table> <p>(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。</p> <p>(五) 資安宣導：2023 年製作三份資安宣導郵件，傳遞資安風險案例與注意事項。</p> <p>(六) 教育訓練：2023 年實施一次員工線上資訊安全教育訓練及考核，與總公司實體資訊安全教育訓練一次。</p> <p>(七) 客戶滿意：無重大資安事件與客戶資料遺失之投訴事件。</p>			每日	系統狀態檢查	每周	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	資訊循環之內部稽核、會計師稽核												
每日	系統狀態檢查																						
每周	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	資訊循環之內部稽核、會計師稽核																						
附件	無。																						