# 資通安全管理

| | |
|---|---|
| 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. 本公司訂定「資訊安全政策」，核決層級為董事會，每年定期檢視或於發生重大變動時重新評估，以符合相關法令，並確保本公司各項資訊資產於各項作業流程中之機密性、完整性、可用性與適法性。<br>2. 本公司設置資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，資訊安全專責主管每季於資訊安全會議中向高階主管報告資訊安全執行情形；每年將前一年度資訊安全整體執行情形，由資訊專責單位主管與董事長、總經理、總稽核及法令遵循主管聯名出具內部控制制度聲明書，提報董事會通過。<br>3. 本公司已參照 ISO27001 國際標準，建立資訊安全管理程序，並於 106 年起導入資訊安全管理系統(ISMS)，並通過「ISO 27001:2013 資訊安全管理系統」國際標準認證，要求各項資訊安全標準，並持續強化資安防護能力。<br>4. 為確保公司資訊資產之安全，公司採用縱深防護架構，將網路分段，透過多層級的安全保護，強化網路安全，持續從物理安全、網路安全、設備安全、作業安全、資料安全等各方面落實安全管理；對外出口，部署網頁應用程式防火牆(WAF)、入侵偵測系統(IPS)等資安設備；區域間接配置防火牆；並部署資料外洩防護系統 |

| | |
|---|---|
| | (DLP)、網頁代理系統(PROXY)等資安設備，並針對網路活動進行 24 小時全面監控。<br>5. 為建立整體之資安意識，所有員工每年接受之資訊安全相關教育訓練基本時數在 3 小時(含)以上，資訊安全專責單位人員每年則至少接受 15 小時以上資訊安全教育訓練，提升員工對資訊安全之認知。 |
| 列明最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實及原因。 | 本公司過去三年並未遭遇重大資訊安全事件，導致營運損失或主管機關裁罰之情形。 |
| 資通安全風險對公司財務業務之影響及因應措施 | 本公司評估資通安全風險對公司之可能影響，除不斷投入資源強化資安防護措施外，本公司亦每年定期執行各項資安通安全演練及測試，如關鍵系統災難備援演練、DDoS 演練、社交工程演練以及網站滲透測試，並委託第三方專案單位辦理電腦系統資訊安全評估，降低資通安全風險。 |