# 資通安全風險管理架構、政策及執行情形

| 項目 | 說明 |
| --- | --- |
| 資通安全風險管理架構 | 本公司重視資訊安全管理，於 2026 年 2 月 24 日經董事會通過訂定「資訊安全維運管理辦法」，並設置資訊安全主管 1 人及資訊安全專責人員 1 人，負責資訊安全相關制度之推動、資訊系統管理與維護，以及資通安全風險之防範與管理。 |
| 資通安全政策 | 本公司依據「資訊安全維運管理辦法」辦理相關資訊安全管理作業，以維護公司資訊資產之機密性、完整性及可用性，降低資訊洩漏、系統異常及營運中斷等風險。 |
| 具體管理方案 | 本公司依據「資訊安全維運管理辦法」執行資訊安全相關管理作業，透過使用者帳號及存取權限管理、防毒軟體與網路安全防護，以及重要資訊與系統資料定期備份、定期資訊安全教育訓練等措施，降低資訊安全風險，維持公司資訊系統之正常運作。 |
| 年度執行情形 | 本公司持續推動資通安全管理及員工資安意識提升，115 年度主要執行情形如下：<br>**一、辦理全員社交工程演練**<br>本公司於 115 年上半年針對全體員工辦理社交工程演練，透過 2 種不同主題之模擬釣魚電子郵件，測試員工對可疑郵件之辨識及防範能力。<br>本次演練共涵蓋 39 人，涵蓋率達 100%，其中 7 人誤點模擬釣魚郵件。<br>**二、演練結果檢討及資安宣導**<br>演練結束後，本公司針對演練結果進行檢討，並對 7 名誤點模擬釣魚郵件之員工安排個別資安宣導及補強教育訓練，強化員工對社交工程攻擊、可疑郵件及惡意連結之辨識能力，以降低資通安全風險。<br>**三、重大資通安全事件**<br>本公司 114 年至 115 年截至揭露日止，未發生對公司財務、業務或營運造成重大影響之資通安全事件，亦無因此遭受重大損失之情形。 |