2.3.2 資訊安全管理

建構韌性營運與數位資產防護體系

重大資安事件	客戶隱私違規事件	五大核心目標
0 件	0 件	全數達成

一、資安承諾與策略願景

在數位轉型與永續發展（ESG）的全球趨勢下，本公司已將資訊安全視為企業韌性的核心基礎，而非單純的技術維護工作。作為循環經濟與資源回收產業的領導者，我們的核心承諾是：

「建構安全且具韌性的營運環境，保護客戶、員工及供應商的資訊資產安全」

資訊安全的落實，直接回應 ESG 架構下兩大關鍵面向：

- **社會責任（Social）：**嚴格保護客戶與員工的個人資料與數據隱私。
- **公司治理（Governance）：**強化內部控制，落實資安風險管理機制。

透過完善的資安體系，本公司確保資源循環過程中的關鍵營運數據不受破壞或竄改，持續保障業務持續性（Business Continuity），並維護各利害關係人對本公司的信任。

二、資訊安全治理架構

本公司建立了權責分明的三層級資安治理組織，確保資安政策由決策高層向下貫穿至第一線作業現場。

「總經理兼任資訊長」的整合式領導模式

整合式領導模式帶來三項具體優勢：

- **策略一致性：**資安決策與業務目標充分協調，確保預算精準投入關鍵防護領域。
- **跨部門協作：**由最高主管主導，有效打破部門壁壘，強化全公司資安聯防。
- **合規保障：**確保資安管理制度符合政府法令與內部控制要求，實現治理與效率的雙重目標。

治理組織與職責分工

治理層級	核心職責
董事會	最高監督單位，每年定期聽取資安執行成效報告，審核整體資安策略目標。
資安管理委員會	由總經理兼任資訊長（CIO）直接領導，負責制定資安政策、核定預算及整體策略規劃，確保資安決策與業務目標高度一致。
資安執行小組	負責落實日常資安政策與技術布局，維護各項防護措施的有效運作。
緊急處理小組	各區域資安緊急應變單位，負責突發事件的即時處置、損害控制與災後系統恢復。

三、資安管理制度：PDCA 持續強化循環

本公司採用 PDCA（規劃 Plan、執行 Do、檢查 Check、行動 Act）管理框架，建立五大核心維度的動態防護體系，確保資安管理能即時回應不斷演變的外部威脅。

人員	推動全員資安意識訓練與定期政策宣導，實施嚴格的「最小權限原則」，確保每位員工僅能存取職務所必要的資訊資產，有效降低內部人為風險。
技術	部署多重技術防護屏障：次世代防火牆、端點防毒系統、定期弱點掃描，以及關鍵資料的異地備份與定期還原演練，確保系統在遭受攻擊後能迅速恢復。
監控	委託外部專業資安業者進行全天候即時監控，結合威脅情報分析，確保任何異常事件均能在第一時間獲得通報與妥善處置。
合規	定期執行內部稽核及委請會計師進行電腦審計，全面檢核各項作業是否符合法律法規與公司制度，確保資安管理體系無漏洞。
風險	主動執行動態風險評估，針對高風險項目與新興外部威脅即時調整防護策略與資源配置，將外部壓力轉化為持續改善的動力。

四、資安風險評估與重大威脅識別

針對資源回收產業的特殊性，本公司識別出五大關鍵風險類別，並持續評估其對業務持續性的潛在衝擊：

詐騙與社交工程	不法分子利用偽造電子郵件誘騙員工執行匯款或提供帳號密碼，威脅公司資金安全。此為最普遍且持續性的威脅類型。
商業間諜與滲透	外部駭客透過進階持續性滲透（APT）技術，企圖竊取製程專利、客戶名單或核心業務機密，對競爭優勢構成長期威脅。
勒索軟體攻擊	犯罪集團植入勒索病毒，加密關鍵營運資料導致業務停頓。此類風險對 24 小時不間斷運作的生產現場威脅性尤為嚴峻。
網路中斷風險	遭受大規模 DDoS 流量攻擊或軟硬體故障，造成核心業務系統或廢棄物追蹤系統停擺，影響正常服務提供。
內部人員風險	員工誤點惡意連結、違規使用外部儲存裝置（如 USB）導致資料外洩，以及離職員工惡意破壞系統資產等情形。

五、資安意識深化：打造全員防護文化

本公司深信，「人」是整個資安防禦體系中最關鍵的第一道防線。再完善的技術系統，若缺乏具備資安意識的員工配合，仍可能因一時疏忽而功虧一簣。為此，我們透過以下三大措施，將資安意識植入日常工作文化：

實戰化教育訓練

每季定期公告最新資安規範，並辦理涵蓋全員的教育訓練課程。訓練採分級設計：一般同仁接受基礎資安通識教育，資訊安全專業人員則接受進階技術培訓，確保不同職能層級的員工均具備相應的防護知識。

針對釣魚郵件進行模擬演練，以量化數據追蹤並持續降低員工「點擊率」，強化全員對社交工程攻擊的直覺辨識能力。

即時威脅通報機制

設立「詐騙郵件通報信箱」，結合時事案例（如「普發補助款詐騙」等社會工程攻擊手法）製作警示通告，透過內部管道即時發送給全體員工，確保防護資訊在威脅發生前第一時間傳達。

社交工程攻擊預防宣導

設立「社交工程攻擊預防宣導」專屬網站，提供員工查詢最新詐騙手法與防範指引的常設資源，將安全文化從訓練課程延伸至日常工作的每一個環節。

六、管理成效與未來展望

於本報告期間，本公司資安管理體系展現出具體且可量化的成效，充分體現「韌性營運」的核心承諾：

核心成效指標	本期成果	對利害關係人的意義
重大資安事件件數	0 件	核心系統全年穩定運作，業務合作夥伴可放心持續合作。
客戶隱私違規事件件數	0 件	客戶敏感資料獲得嚴密保護，維繫企業商譽與信任關係。
五大核心目標達成情況	全數達成	涵蓋系統有效性、資訊資源保障、資產安全、法規合規、關鍵業務持續經營。

展望未來，本公司將持續深化 PDCA 管理循環，積極因應 AI 驅動攻擊、供應鏈資安風險等新興威脅，並評估導入 ISO/IEC 27001 資訊安全管理系統認證，進一步強化資安治理的國際公信力，為所有利害關係人提供更堅實的數位資產保障。