樂事綠能科技股份有限公司

資通安全風險管理作業

一、目的:本公司依據「公開發行公司建立內部控制制度處理準則」，為控制資訊通訊使用之安全及風險為目的，成立資訊安全風險控制推動小組，綜理全公司資通安全環境建置、風險評估、鑑別及防範，並訂定資通安全政策及推動以符合外部議題及利害關係人對本 公司之資通安全要求與期望，確保本公司資訊、通訊取得安全及使用處於完整、可用及保有機密性。

二、資通安全對象及適用範圍

對象：包括員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。

範圍：公司用以營運目的之機器設備及配有作業系統、連接或使用網路、儲存媒體及應用系統和供應此設備系統、服務之廠商、客戶等，資訊安全風險控制推動小組進行資訊安全制度之規劃、監控及執行資訊安全管理作業。

三、資通安全架構

資訊安全風險控制推動小組設置資安長一名,資安專責主管一名及資安人員一名並以各部門主管為主要成員，負責資訊安全政策的推動及執行，並以執行情形檢討修正資訊安全制度，每年定期向董事會報告。

四、資通安全政策目標

資通安全政策的主要目標是關注安全管理，法律合規和資產保護三個方面，從系統到技術， 從人員到組織，全面提高安全防護能力，避免資訊遭受竊取、竄改或服務中斷，影響公司商譽。

鑑於當前資產安全的新趨勢，如 DDoS（分散式阻斷服務）攻擊，勒索軟體，社交工程、釣魚郵件和虛假網站，尋求外部資源(支援)協助資安演練及弱點偵測，不定期舉行資安教育訓練。

五、資通安全控制措施

預防控制:

1.定期盤點資訊設備，
2.定期資料備份控制
3.復原程序演練
4.修復程式安裝，注意韌體及作業系統安全更新。
5.網路分段設置、VPN 建置
6.建置防火牆政策設立

偵測控制:

1.防毒軟體安裝，病毒碼更新控制
2.入侵防禦軟體、弱點掃描作業

矯正控制:

1.事件影響計劃:

隔離感染設備、進行診斷(病毒、勒索…)、資安通報、進行分析(途徑、原因、方式)、執行遏制、根除、影響、資料回復、更換金鑰憑證、執行漏洞掃描、硬體修正、上線、執行額外的漏洞掃描、滲透測試。

2.回復程序

六、相關文件

資通安全檢查作業　　CG9007