資訊安全風險管理架構暨政策與管理方案

一、資訊安全風險管理架構

本公司資訊系統是向關係人「利華羊毛工業股份有限公司」租用，該公司有設置資訊副理負責督導內部資訊安全執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體作為，且定期持續追蹤改善成效，以降低內部資訊安全風險。

二、政策

1. 台北總公司與屏南廠皆建立設置妥善防火牆，以阻擋外部駭客之攻擊，並不定時檢閱相關記錄檔。
2. 電腦用戶端部署安裝防毒軟體，並不定時檢閱病毒記錄及相關對應處理。
3. 不定時不定期進行作業系統更新相關作業，減少系統漏洞而降低資訊安全風險。
4. 建立妥善的備份機制與方式。

三、管理方案

1. 網路安全管理：
   I. 對外連線設置企業級多功能防火牆，以防止駭客非法入侵。
2. 伺服器或電腦用戶端防護管理：
   I. 伺服器與電腦用戶端設備內均安裝有端點防護多功能軟體(防毒、防惡意程式、防間諜程式…等)，病毒特徵碼採取自動更新方式，確保能阻擋並提升各類病毒或資訊安全防護。
   II. 電子郵件設置有郵件防毒、垃圾郵件過濾機制及反勒索詐騙的郵件防禦機制，以防堵上述類別惡意郵件被電腦用戶端收下後，造成不可預期的損失或危害。
3. 應用系統使用者帳號權限管理：
   I. 帳號管理，系統設定要求使用者需定期進行密碼變更。
   II. 權限管理，依不同使用者職務屬性定義其可使用權限。