世紀民生科技股份有限公司

資通安全政策、風險架構、政策目標及資安控制措施

(一). 執行情形(114 年)：

持續執行汰換舊電腦主機及 windows 系統升級作業，宣傳資訊安全及相關資訊給員工。

114 年 11 月 28 日舉辦「電子郵件社交工程介紹與防護」教育訓練。

共 11 人參加，占員工 12 人比率 91.97%。

鼓勵資訊人員參加資訊安全相關講座，獲取資訊安全資訊。

(二). 資訊安全政策

為揭示本公司對資訊安全之重視，建立資訊安全管理機制以確實掌握資訊設備及網路安全，保障公司作業電腦化規劃及資料處理之機密性、可用性及完整性，當資安風險或緊急事件發生時，本公司具體應變處置原則及能力，以確保業務迅速恢復正常運作特定資訊安全政策。

1. 對象：本公司全體同仁及其他得接觸本公司業務相關資訊之合作夥伴、委外廠商。

2. 範圍：本公司所有資訊資產，或其他本公司未實際所有，但基於合約、法律及法規所賦予之責任而可支配之資訊資產。

(三). 資訊安全風險架構

本公司資訊安全由蔡瑞遠擔任資安專責主管及帶領1名資安專責人員，來負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關資訊安全作業；綜理資訊安全政策推動及資源調度事務，定期檢討修正「資訊安全政策」、每年執行情形，以確保公司、客戶機密資訊不外漏、公司業務永續運作。另外，為強化企業資安聯防，資安專責主管已加入台灣電腦網路危機處理暨協調中心(TWCERT)以共享資安情資。

稽核室將「資通安全檢查作業」納入年度稽核計劃進行查核作業，受稽單位並依照缺失進行改善及追蹤，以落實公司資訊安全政策。
114年度進行查核作業，無發生缺失改善需追蹤之情事。

(四). 資訊安全政策目標

建立安全及可信賴之資訊作業環境，確保資訊資產之機密性、完整性及可用性，並提昇同仁對資訊安全認知，以保障員工、客戶與本公司之權益。

(五). 資訊安全控制措施

項目	具體作為
防火牆防護	防火牆設定連線規則。 如有特殊連線需求需額外申請開放。 監控分析防火牆數據報告。
使用者上網控管機制	使用自動網站防護系統控管使用者上網行為。 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	使用多種防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	作業系統自動更新，因故未更新者，由資訊部協助更新。
資訊備份機制	重要資訊系統資料庫皆設定每日完整備份、每小時差異備份。 定期執行資料回復演練。
異地存放	伺服器與各項資訊系統備份檔，分開存放子公司。
資訊中心檢查紀錄	資訊中心檢查資料備份、防毒軟體更新等。
資安聯防	申請加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)作為資安情資分享、資安宣導活動之來源管道。
教育訓練	定期進行全體員工資安教育訓練提升員工資安意識。