皇普建設股份有限公司
資訊安全政策及管理作業程序

108.10.01

第一條：資訊安全風險架構

一、本公司資訊安全之權責單位為行政服務部，負責統籌資訊安全及相關事宜，並定期進行內部資訊安全檢查。

二、本公司稽核室為資訊安全監理之督導單位，負責擬定相關內部控制程序管理及督導內部資安執行狀況，若查核發現缺失，立即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。

第二條：資訊安全政策

一、目的

為建置本公司安全及可信賴的資訊運作環境，維持業務持續運作，降低資訊作業風險，以達成資訊安全管理的目標。

二、範圍

包括本公司所屬各據點資訊作業之硬體、軟體、服務、文件及人員。

三、目標

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

四、程序

執行資訊機房、網路安全、資料安全、資訊保密、資訊委外等管理。

第三條：資訊安全管理措施

一、權限管理

制定人員帳號、權限管理與系統操作行為之管理措施，並落實人員帳號權限管理與審核。

二、外部威脅

強化內部潛在弱點、中毒管道之防護措施，定期執行主機電腦弱點檢測及更新，並做病毒防護與惡意程式檢測。

三、系統可用性

系統可用狀態與服務中斷時，維持系統網路可用狀態監控及通報機制、資訊備份機制並定期災害復原演練。

第四條：作業內容

一、事前預防控制

(一)環境管理：強化資訊環境安全管理、加強防火牆系統。

(二)資料管理：應用資料加密系統、權限管控系統、加強管理管制資料存取。

(三)人員管理：定期辦理資訊安全教育訓練，不定期推播及宣導資訊安全。

二、即時問題處理

(一)環境回復：透過復原計畫，逐步回復服務。

(二)資料復原：透過備份系統，將資料復原。

(三)快速處理：透過短期對策，縮短影響時間。

三、事後檢討

(一)紀錄過程：事件處理過程詳細紀錄，並作長期對策，防止再發生。

(二)保留證據：保留證據，調查事件始末。

(三)教育訓練：藉由資安事件加強員工資安及風險管理。

第五條：資訊安全強化方案

一、陸續導入多項資安措施，提升整體資訊安全

(一)提升資訊防禦能力：升級防毒防駭系統、加強防火牆系統。

(二)降低資料損失風險：建立異地備份機制。

(三)建立軌跡紀錄功能：導入資料存取稽核系統。

二、未來資訊安全規劃

(一)定期執行系統安全漏洞掃描。

(二)持續強化基礎資訊環境。

(三)建立備份資料異地存放機制自動化。

第六條：附則

本作業程序經總經理核准後施行，修正時亦同。