裕民航運

目標	風險	控制點	風險等級	自評分數
確保系統及資料安全，不被輕易破壞。	若無控制將造成資訊系統輕易被侵入破壞。	一、防止不明人士入侵破壞：防火牆機制的建立，並隨技術的更新，不斷提昇防止駭客及不法人士入侵的防範機制。	1.36	4.55
	系統遭病毒侵入破壞，使系統當機或毀損。	二、避免病毒傳遞入侵為害：1.防止病毒的入侵，安裝防毒軟體做第一道已知病毒防護，進入郵件伺服器的 E-mail 會先過濾。2.PC 安裝使用者端防毒程式。3.建制對 E-mail 的附加檔案限制，針對特殊危險的附加檔名過濾，以因應病毒的不斷更新。	1.36	4.45
	相關系統資料被竊取外洩。	三、相關系統登錄密碼管制：依據公司資訊控制管制要點所定密碼管理規則，於伺服器建立控管機制，使用人依規定使用，否則無法登錄。	1.27	4.64
		四、系統使用權限的管制：系統使用的權限，包括資料的顯示及報表的輸出，皆須依管理單位所核准的人員及其權限做嚴密的控管，以防資料的外洩。	1.27	4.55