宜特資訊安全風險及管理措施

1. 資安風險評估分析

茲因科技進步與通訊發達，為強化保護宜特科技與客戶文件資產，宜特科技進行內外環境因子檢視。外部風險為:網路攻擊威脅、駭客入侵。內部風險為資訊外洩、中毒、機房管理。

2. 因應措施

(1) 透過安全管控委員會，整合各部門進行安全管理程序運作，並針對安全事件進行有效管理與預防再發，期望降低資安風險發生之可能。

(2) 宜特科技內部建立了各項管理措施，諸如：防毒軟體、WSUS、防火牆管理、VLAN 管理、VPN 管理以及各項機台設備的管控機制，但無法保證這些措施可以完全避免來自任何第三方惡意的攻擊。但會透過異地備援、機房與網路 HA(High Availability)架構以及每年的災難復原演練，並檢視與評估內部程序，確保系統運作的適當性與有效性。

(3) 宜特科技可能面臨電腦病毒、及具有破壞性、勒索性的軟體、或是因為員工無意或是惡意行為，進而造成客戶的資料外流或是損害。有鑑於此，宜特科技內部也透過導入文件加密軟體，進而保護客戶之實驗條件、結果、報告等檔案。

(4)為強化資訊安全管理架構，宜特科技於民國一零九年十月取得 ISO27001 認證通過，並透過下列制度但不限於：系統弱點掃描與修正、社交攻擊演練、日誌管理與分析等，確保資安事件偵測的有效性。

(5)即便在各項層面都盡力完成設施與建立制度，但不能保證宜特科技在日新月異的資訊安全威脅環境中，仍可以時時刻刻保有各項資訊的機密性、完整性與可用性。若宜特科技無法即時解決網路攻擊所造成的技術性上的問題，有可能會造成宜特科技資訊系統與環境的異常或是損害，進而損及宜特科技對於客戶以及其他利害關係人之承諾，並可能導致宜特科技營運成果、財務狀況、前景與聲譽因此遭受重大之不利影響。