宜特信息安全风险及管理措施

1. 资安风险评估分析：

兹因科技进步与通讯发达，为强化保护宜特科技与客户文件资产，宜特科技进行内外环境因子检视。外部风险为:网络攻击威胁、黑客入侵。内部风险为信息外泄、中毒、机房管理。

2. 因应措施：

(1) 透过安全管控委员会，整合各部门进行安全管理程序运作，并针对安全事件进行有效管理与预防再发，期望降低资安风险发生之可能。

(2) 宜特科技内部建立了各项管理措施，诸如：防病毒软件、WSUS、防火墙管理、VLAN 管理、VPN 管理以及各项机台设备的管控机制，但无法保证这些措施可以完全避免来自任何第三方恶意的攻击。但会透过异地备援、机房与网络HA(High Availability)架构以及每年的灾难复原演练，并检视与评估内部程序，确保系统运作的适当性与有效性。

(3) 宜特科技可能面临计算机病毒、及具有破坏性、勒索性的软件、或是因为员工无意或是恶意行为，进而造成客户的数据外流或是损害。有鉴于此，宜特科技内部也透过导入文件加密软件，进而保护客户之实验条件、结果、报告等档案。

(4) 为强化信息安全管理架构，宜特科技于民国 109 年 10 月取得 ISO27001 认证通过，并透过下列制度但不限于：系统弱点扫描与修正、社交攻击演练、日志管理与分析等，确保资安事件侦测的有效性。

(5) 即便在各项层面都尽力完成设施与建立制度，但不能保证宜特科技在日新月异的信息安全威胁环境中，仍可以时时刻刻保有各项信息的机密性、完整性与可用性。若宜特科技无法实时解决网络攻击所造成的技术性上的问题，有可能会造成宜特科技信息系统与环境的异常或是损害，进而损及宜特科技对于客户以及其他利害关系人之承诺，并可能导致宜特科技营运成果、财务状况、前景与声誉因此遭受重大之不利影响。