

宜特信息安全具体管理方案及投入资源

资安防护措施	
强化人员知能	加强同仁资安意识：新人到部当天须完成新人信息安全教育训练，之后每人每年度须进行回训。
	强化资安意识：不定期发送资安电子报或是资安公告，协助同仁掌握资安规范以及了解外界资安攻击样态，111年度发送14封。
	社交攻击演练：每年举行两次社交攻击教育训练，并举办一次钓鱼信件测试，验证同仁资安意识。
	尊重知识产权：禁止使用非法或是破解、免安装软件。
	提升资安技能：指派资安技术人员，不定期参加外部资安工具训练或是黑客攻防技术课程，以加强资安素养与技能，111年度共计26人次。
避免数据外泄	文件加密：导入文件加密软件，妥善保护与降低机密数据文件外泄机会。
	权限控管：档案操作依照必要性进行访问权限设定并定期检讨。
	网络管理：对网络流量异常进行警示与查核、对外传输数据，必须经过申请核准。
	存取管制：禁止携入私人储存装置、禁止私人设备进行拍照或录像、USB port禁止使用储存装置。
落实日常维运	查核与改善：定期进行系统查核与改善，导入新技术来加强数据防护。透过定期内部稽核以及外部资安验证单位稽核，确保符合管理制度要求，111年度内部稽核1次、外部验证稽核1次、信息安全执行小组每月举行检讨会议。
确保服务可用	备份管理：重要系统进行备份管理，依照年度计划新购或是升级资安。111年度完成一次备份还原测试。
	资安防护：为强化内外部网络攻击防护，进行防火墙政策调整与审核、启动网络入侵检测、防毒系统定时更新、漏洞修补与维护。对重要主机加强防护，导入微分子防火墙，强化横向防御。加入科学园区资安信息共享与分析(SP-ISAC)资安联防，接收重大情资分享。111年度完成一次弱点扫描与并尽可能修复信息系统漏洞。