宜特資訊安全具體管理方案及投入資源

資安防護措施	
強化人員知能	加強同仁資安意識：新人到部當天須完成新人資訊安全教育訓練，之後每人每年度須進行回訓。
	強化資安意識：不定期發送資安電子報或是資安公告，協助同仁掌握資安規範以及了解外界資安攻擊樣態，111年度發送14封。
	社交攻擊演練：每年舉行兩次社交攻擊教育訓練，並舉辦一次釣魚信件測試，驗證同仁資安意識。
	尊重智慧財產權：禁止使用非法或是破解、免安裝軟體。
	提升資安技能：指派資安技術人員，不定期參加外部資安工具訓練或是駭客攻防技術課程，以加強資安素養與技能，111年度共計 26 人次。
避免資料外洩	文件加密：導入文件加密軟體，妥善保護與降低機密資料檔案外洩機會。
	權限控管：檔案操作依照必要性進行存取權限設定並定期檢討。
	網路管理：對網路流量異常進行警示與查核、對外傳輸資料，必須經過申請核准。
	存取管制：禁止攜入私人儲存裝置、禁止私人設備進行拍照或錄影、USB port禁止使用儲存裝置。
落實日常維運	查核與改善：定期進行系統查核與改善，導入新技術來加強資料防護。透過定期內部稽核以及外部資安驗證單位稽核，確保符合管理制度要求，111年度內部稽核1次、外部驗證稽核1次、資訊安全執行小組每月舉行檢討會議。
確保服務可用	備份管理：重要系統進行備份管理，依照年度計畫新購或是升級資安。111年度完成一次備份還原測試。
	資安防護：為強化內外部網路攻擊防護，進行防火牆政策調整與審核、啟動網路入侵偵測、防毒系統定時更新、漏洞修補與維護。對重要主機加強防護，導入微分子防火牆，強化橫向防禦。加入科學園區資安資訊分享與分析(SP-ISAC)資安聯防，接收重大情資分享。111年度完成一次弱點掃描與並盡可能修復資訊系統漏洞。