編　號	作　業　項　目	作　業　程　序　及　控　制　重　點	依　據　資　料
CC-110	資通安全檢查作業	一、目標： 1、針對軟硬體設備及與財務報告系統及其相關子系統制定資訊安全政策。 2、定期實施資訊安全檢查作業，落實資通安全政策，以確保資通安全無虞。 二、權責單位：資訊部 三、潛在風險： 1、資訊安全控制是否依據整體財務報告系統及其相關子系統之資訊架構進行全盤量。 2、員工資訊安全意識及技能是否有效落實資訊安全政策。 3、資通安全檢查機制及規範是否適當，確保資訊安全檢查作業之有效遵行。 4、未依資訊安全政策執行檢查，將無法確認資訊安全政策之有效落實 四、控制重點： 1、應安裝防火牆及防毒軟體並定期更新病毒碼。 2、應無法使用盜版軟體，無法任意從網際網路下載不明軟體進行安裝。 3、電腦軟體登入密碼應定期更換。 4、應確保資訊安全檢查或資訊安全宣導有效執行。	1、使用表單： (01)SSL-VPN 申請單

編　號	作　業　項　目	作　業　程　序　及　控　制　重　點	依　據　資　料
CC-110	資通安全檢查作業	五、作業程序： (一)電腦系統安全作業 1、電腦軟體設計定期作系統檢查及維護。 2、電腦軟體設計皆保存系統流程圖、檔案結構說明及系統操作說明。 3、遠端連線應事先提出申請，使用「SSL-VPN 申請單」，並可紀錄存取進出的使用者 ID、登入時間。 4、應安裝防火牆，定期更新電腦作業系統的補強程式及防毒系統的病毒碼。 (二)備份作業 1、每日檢查當天凌晨備存作業是否完成並且沒有任何錯誤，同時填寫備存紀錄單將備存作業結果詳細紀錄，並定期更換備存磁帶。 2、定期由專人把備份完成的磁帶作異地保管。 (三)相關報表網路接收暨系統查詢作業 1、有專人管理電子郵件系統登入系統皆需密碼認證，遇使用者離職或異動時都需填單並立即變更密碼或刪除登入權限。 2、電腦軟體登入都需密碼控管，依職責設定權限，並可由使用者自行定期更換密碼。 (四)資訊安全政策落實 1、每位員工均須填寫保密協定，不可洩露個人職務上的機密資料。 2、不定期依資訊安全政策執行資訊安全檢查，以有效落實資訊安全政策。 3、不定期利用 MAIL 或其他管道宣導資訊安全要求事項。	