

項目	(七) 資通安全防護及控制措施		
7.19	是否訂定資訊處理設備作業程序、變更管理程序及管理責任 ( 如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等 )，且落實執行？是否訂定資訊設備回收再使用及汰除之安全控制作業程序，以確保任何機密性或敏感性資料已確實刪除？		
稽核 依據	資通安全管理法施行細則第 6 條： 資通安全防護及控制措施		P8
	1. 資通安全管理法施行細則第 6 條第 1 項第 8 款：資通安全防護及控制措施 2. 資通安全責任等級分級辦法第 11 條第 2 項： (1) 資通系統防護基準之系統與通訊保護-傳輸之機密性與完整性(資通系統高等級者) (2) 資通系統防護基準之系統與資訊完整性-軟體及資訊完整性 3. CNS27002：2023 7.8 設備安置及保護、7.13 設備維護、7.14 設備汰除或重新使用之保全、 8.技術控制措施 8.32 變更管理資訊處理設施及資訊系統之變更，宜遵循變更管理程序。		
稽核 重點	應就資訊處理設備訂有作業程序	佐證 資料	資訊處理設備作業程序、變更管理程序、設備移除 ( 報廢 ) 紀錄
稽核 參考	下列安全措施提供參考： 1. 機關資訊處理設備，應至少包括個人電腦、伺服器、網路設備、資安防護設備等。 2. 資訊處理設備作業程序，應至少包含新增、異動及移除 ( 報廢 ) 程序，並應含管理權責及相關變更作業程序。 3. 對機密與敏感性資料之儲存媒體實施防護措施，例如 ( 但不限於 ) 儲存於加密磁碟、置於上鎖之機櫃等。 4. 設備安全處理程序 ( 包括報廢程序 ) 及分級標示。 5. 資訊及資通系變更程序應包含設備回收或再利用規範。 6. 資訊設備刪除或汰除前應先逐一確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。 7. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、		

	刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。
FQA	