

**勞動部勞工保險局「115 年數位服務整體營運環境再造案」公開閱覽文件  
廠商意見回覆彙整表(雲杉科技股份有限公司)**

(註:本案意見回覆僅供參考，各項修正具體內容及文字，以正式公告之招標文件為準。)

項次	章節	頁次	公開閱覽文件內容	廠商疑義	廠商建議修改	本局回復說明
1	建議書徵求說明書參、二、(一)	31 頁	將本局所需加密分持之資料(含現行核心系統之全量資料)放置於資料收集設備，並將備份檔案進行高安全性加密(ASE-256)分持，加密分持檔案皆須透過專線進行傳輸，使用時由廠商租用	其中 ASE-256 應為誤植，正確演算法為 AES-256		納入 RFP 修改參考。
2	建議書徵求說明書肆、二、(二)	69 頁	18、須具備資料(含資料庫資料表格空間檔案系統)存放完整加密功能及資料庫之表格與欄位加密功能，以維護機敏資料，防止人為竊取資料。資料於網路傳輸及備份時，亦須可針對資料加密。	資料加密金鑰是否應儲存於本案之硬體安全模組內？。	『須具備資料(含資料庫資料表格空間檔案系統)存放完整加密功能及資料庫之表格與欄位加密功能，且加密金鑰受本案之硬體安全模組保護，以維護機敏資料，防止人為竊取資料。資料於網路傳輸及備份時，亦須可針對資料加密。』	1.維持原草案內容。 2.補充說明：本項為本專案需求。

項次	章節	頁次	公開閱覽文件內容	廠商疑義	廠商建議修改	本局回復說明
3	建議書徵求說明書肆、七、(二)	83 頁	F. 支援備份資料加密功能，採用 AES-256 加密方式，並符合 FIPS 140-2 安全規範，支援資料安全刪除功能，符合 NIST SP 800-88 規範，支援資料傳輸加密功能	資料加密金鑰是否應儲存於本案之硬體安全模組內？	『支援備份資料加密功能，採用 AES-256 加密方式，加密金鑰受本案之硬體安全模組保護，支援資料安全刪除功能，符合 NIST SP 800-88 規範，支援資料傳輸加密功能。』	1.維持原草案內容。 2.補充說明：本項為本專案需求。
4	建議書徵求說明書肆、十四、(二)	151 頁	(1) 為確保系統運作相容與穩定性，廠商所提供的硬體安全模組及金鑰管理系統須來自同一個品牌的解決方案之組合。	請教『同一品牌的解決方案』之定義，是否為『同一原廠的原廠解決方案』或有其他定義？	1. 若是，原廠是否需要提具原廠出廠證明，金鑰管理系統是否需要 FIPS 認證？建議修改為『為確保系統運作相容與穩定性，廠商所提供的硬體安全模組及金鑰管理系統為同一原廠之解決方案組合。』 2. 若不是，建議要求改為『為確保系統運作相容與安全性，廠商所提供金鑰管理系統須使用 PKCS#11 API 呼叫同一作業系統內原廠 SDK 透過雙向憑證認證之加密通訊直接與硬體安全模組通訊以取消中間人攻擊機會，金鑰須直接儲存於硬體加密模組內以降低外洩之可能性。』	納入 RFP 修改參考。

項次	章節	頁次	公開閱覽文件內容	廠商疑義	廠商建議修改	本局回復說明
5	建議書徵求說明書 肆、十四、(二)	151 頁	(15) 須提供至少兩個 Gigabit Ethernet 介面。	本案例其餘設備與伺服器均要求有配置 SFP 光纖網路介面，僅此設備不要求配置光纖介面，建議對此設備亦要求配有光纖網路介面以統一設備連線要求。	『須提供 2 埠(含)以上 10Gbps 光纖網路介面。』	1.維持原草案內容。 2.補充說明：本項為本專案需求。