中小企業數位共好計畫

計畫管理可視化戰情室維運需求書

壹、目的

本組執行經濟部中小企業處之中小企業數位共好計畫，目的為協助我國小微型企業數位賦能，導入新興科技應用，促進企業經營管理效率及優化服務流程體驗…等。為掌握小微型企業雲端工具需求、導入成效及發展趨勢，同時持續維護平台之功能優化及擴增等相關功能，擬規劃計劃管理可視化戰情室維運。

貳、系統功能需求

一、 內容需求

1. 資料儲存彙整，推動數據資料數位化，計畫關鍵指標與數據連動，每年約3,000筆資料。
2. 儀錶板，需可呈現專案計畫所需資訊儀表板。
3. 計畫數據分析，精進系統自動化統計公式、檢核及特殊資料轉碼等功能，針對小微型企業雲端工具需求、導入成效及發展趨勢等相關計畫資訊進行分析。
4. 小微卡及多項計畫問卷資料交叉比對，並連動計畫數據，以進行質化、量化多重分析及趨勢分析。
5. 圖表產製，依照計畫需求及主題化需求進行多維度分析，並產製一般圖表及客製化圖表，如輪廓分析圖表及多維度分析視覺化統計圖表等。

二、功能需求

1. 針對平台需求盤點評估，並提出評估報告書：使用者需求面、視覺設計面、使用者友善性、後台設置權限…等。
2. 批次匯入、匯出資料表功能需支援多項資料格式，如XML、CSV、RDF、試算表等。

3. 儀錶板設計及結果顯示。
4. 資料管理平台設計與管理,需考量產製統計圖表(系統後台產製分析報表如折線圖、長條圖、圓餅圖、地圖等，依計畫資料需求提供)、批次匯出入資料、搜尋/統計/分析、儀錶板發佈…等功能，並保有後續擴充性。
5. 資料表搜尋功能(列出特定欄位內含有搜尋文字的資料）。
6. 多層、多維度分析視覺化統計報表(交叉圖表）。

三、平台規格需求

1. SSL加密：平台導入SSL加密設計。
2. 程式設計介面應採用標準網路協定如HTTPS、SOAP、Web Services、JSON和XML等，以便於日後系統擴充功能時，能與外部系統、資料庫，進行跨系統間之介接。
3. 提出平台代管空間設備說明及租用證明

四、平台維運需求

1. 平台採雲端存取，網站式平台，須相容於一般使用者常用之瀏覽器，包含Microsoft Edge 、Google Chrome、Firefox、Opera、Safari 等瀏覽器，並需確保可以螢幕最佳解析度來呈現網頁。
2. 系統權限控管採多人維護機制，採階層式架構賦予權限和新增使用及相關使用者之權限。
3. 須採開放式、模組化與元件化架構設計，應用程式設計介面，應採用標準網路協定，以因應未來彈性擴充與快速調整，便於後續系統維護及業務發展需求。
4. 搜尋紀錄追蹤(log）。

五、其他配合事項

1. 須提供資安報告，並排出中高風險必須為0。
2. 須配合本會提供需求書、評核機制及提供檢測報告。
3. 驗收文件
   a. 維運需求書、功能測試報告、原碼檢測報告
   b. 系統安裝手冊（系統說明文件及技術文件、系統安裝及備份程序）

可朝向以下功能提供系統規劃與平台整合建議書：

項目	功能	需求說明
平台視覺	視覺	需考量PC及行動平台觀看之需求(RWD)
	字體	統一使用微軟正黑體
	文字格式	項目為金額時，文字格式需加入分位號。項目為百分比時，取至小數點第二位四捨五入。
資料匯出、匯入管理	批量資料匯入	需支援多項資料格式匯入，如Excel(XML)、CSV、試算表等。
	批量資料匯	需支援多項資料格式匯出，如Excel(XML)、CSV、PDF、試算表、

	出	word(doc)等。
	圖匯出	需支援多項『圖片』格式匯出，如 JPG 等
	表匯出	需支援多項『表格』格式匯出，如 Excel(XML)、CSV、PDF、試算表、word(doc)等。
儀表板設計及結果顯示	儀表板設計及結果顯示	需呈現：計畫團隊總數量、數位普及數量、企業上雲數量、數位共融數量、小微企業總數量、縣市、行業別、方案類別。 統計繪製圖表：折線圖、長條圖、圓餅圖、複合圖、文字雲、表格…等能輔助決策圖式化之結果顯示。
資料分析及圖表產製	多表單勾稽	會有多項表單來源：(1)計畫基本資料(2)計畫問卷(3)活動問卷等。各來源表單須可互相勾稽(統一編號)。
	資料呈現	所有欄位皆須編輯且需有獨立輸入兼下拉式選單，且資料表可擴充欄位，並納入資料篩選項目，呈現於圖表。
	圖表編輯	項目顏色、字型可調整更改
	多維度分析視覺化統計圖表(交叉表)	須至少 5-7 欄位項目的交互分析(如年度、資料來源、原住民區、縣市與行業別及政府投入輔導金額之分析)，且需呈現圖、表，如下圖。
資料表搜尋功能	關鍵字搜尋	系統圖表可使用關鍵字去搜尋相關資料數據
資料建置	代碼轉換	縣市及行業(大小類)等欄位資料代碼轉換。
	資料分區	縣市欄位數據須另導出區域(北、中、南、東、外島)
	資料篩出	須從地址欄位篩選出行政區，並呈現行政區欄位。
	篩選器	1. 基本篩選：年度、資料來源、日期區間(須可用月曆勾選時間區間) 2. 特殊篩選：將提供原住民及(山地原住民鄉、平地原住民鄉)、客家(臺三線、六堆、臺九線)及偏鄉區域清單，帶入系統後供篩選原住民區或客家區各鄉數據分析。
	資料排名、序	各欄位須有排名、序功能(需有剔除重複資料功能)
圖表呈現	基本圖	每一欄位至少須有圓餅圖、長條圖、折線圖及雷達圖等選擇呈現。
	基本表	至少須能 5-7 欄位項目交叉分析之多維度交叉表單
	特殊圖	1. 區域相關欄位(如縣市、行政區或原民客家區域等)須有地圖及泡泡圖呈現。 2. 輔導團隊、行業別、雲端供應商、雲端工具及方案類型欄位須要呈現關鍵字篩選之文字雲圖示
安全性	系統管理	操作記錄管理、登入位址管理、登入 log 紀錄、系統維運頁面(系統維修中頁面)
	風險管理	面對惡意攻擊之應對機制
	資安與個資	須符合政府相關規定並提供相關報告
	備援機制	須具備備份備援機制

參、需求時間

111年12月09日前。

肆、預算

預算總上限為新台幣 160 萬元（含稅）。

附件、中華軟協資通系統防護基準

分類	安全需求項目	說明
存取控制	資通系統閒置帳號應禁用。	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。
存取控制	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。	會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，使用者於系統中若一段時間未進行活動，系統應有自動機制將該使用者的會談階段設為失效而登出系統，以降低資安風險。
存取控制	應依機關規定之情況及條件，使用資通系統。	應依據機關規定之情況及條件(如特定時間或指定IP來源等)，限制系統使用行為(如僅開放平時上班時間使用系統、特定功能或機敏資訊僅允許透過內部網路存取等)。
存取控制	遠端存取使用者之權限檢查作業應於伺服器端完成。	應於伺服器端實作權限檢查機制，並預設禁止任何未通過權限檢查之存取行為，以避免被使用者繞過。
存取控制	遠端存取應採用加密機制。	遠端存取資通系統時，應以加密機制保護機敏資料傳輸時之機密性。常見作法如採用HTTPS加密傳輸等，並選擇高強度之協定版本及演算法。
系統與服務獲得	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的finally陳述，確保將該段功能程式碼所使用的資源正確釋放。
系統與服務獲得	資通系統相關軟體，不使用預設密碼。	系統相關軟體元件或組態設定若有使用預設密碼，應於系統正式上線前變更完畢。
系統與服務獲得	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	可參照「安全軟體設計參考指引」之第3章安全軟體設計階段實務活動，包含「安全設計原則」，進行系統設計時應參考使用的設計原則；「執行攻擊面分析」，進行攻擊面的定義、識別與對應方式，包含如

		何進行攻擊面的衡量與評估，並進行管理等；「執行風險分析」，軟體設計過程中，如何透過使用威脅建模與架構風險分析，進行系統架構與威脅的分析，並使用通用性的安全設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連安全軟體設計的實務活動之後，應確保安全設計符合需求階段提出的相關安全需求及安全設計，以符合軟體安全的基準線。
系統與服務獲得	將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	系統發展生命週期需求階段發展之安全需求檢核項目，可能未能充分符合系統之所有安全需求，故應依據風險評估結果進行修正。
系統與服務獲得	應注意避免軟體常見漏洞及實作必要控制措施。	軟體開發時應避免常見漏洞，如OWASP TOP 10或CWE/SANS TOP 25等，這些錯誤容易被惡意攻擊者利用，造成資料被竊取、竄改或使軟體無法運作，故需實作必要控制措施，以降低資安風險。
系統與服務獲得	執行「弱點掃描」安全檢測。	弱點掃描係利用自動化工具，對受測目標進行安全性掃描，以找出系統潛在弱點。
系統與服務獲得	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評估，正面表列需要開啟該服務及埠口之理由，並關閉不必要之項目。
系統與通訊保護	使用公開、國際機構驗證且未遭破解之演算法。	若使用自行創造的加密方式且未經過適當的驗證程序，可能存在設計瑕疵，增加被破解的風險。應採用公開、國際認可之演算法，如AES對稱式加密演算法、RSA非對稱式演算法及SHA-256以上之雜湊演算法等。
系統與通訊保護	加密金鑰或憑證週期性更換。	產生網站HTTPS使用之憑證，應具備使用年限限制，並於到期前進行更換。系統若另行使用自行產生之加密金鑰，亦需定期更換。
系統與資訊完整性	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	對於使用者輸入欄位資料應檢查是否符合預期之邏輯規則，實務上，以正規表示式(RegularExpression)驗證內容之合法性。檢查機制若於客戶端實作，容易被使用者繞過檢查機制，故應於應用系統伺服

		器端實作始視為有效。
系統與資訊完整性	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	針對系統所使用的外部元件與軟體進行表列，包含其版本資訊，定期關注元件版本更新訊息及安全漏洞通告，若有相關之安全漏洞，評估系統元件更新之必要性，並於系統測試環境進行更新測試驗證後，才於正式環境進行更新。
識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	資通系統應具備唯一識別及鑑別使用者之功能，如為內部使用者建立個別帳號，以強化系統之可歸責性。多人共用帳號行為會造成難以藉由日誌識別使用者身分。
識別與鑑別	資通系統應遮蔽鑑別過程中之資訊。	資通系統身分鑑別頁面中，資料輸入欄位(如密碼等)應設定不以明文顯示方式，如以*取代真實輸入字元，以避免他人從旁窺視而盜取密碼。
識別與鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	密碼不可以明文方式儲存，應經過加密或雜湊處理，使得系統管理者或是惡意入侵的攻擊者皆無法輕易取得使用者原始密碼，以降低密碼外洩風險。實務上，當使用者設定密碼時，應針對該帳號產生一個亂數值(Salt)，將密碼結合亂數值，再以雜湊函式處理產生雜湊值後，分別於不同欄位儲存亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。
識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序）。	資通系統若開放給外部使用者(含其他機關、委外開發與維護廠商、臨僱人員及一般民眾等)存取使用，應具備識別及鑑別之能力，如利用帳號、憑證或來源IP位址等方式，識別與鑑別使用者。
識別與鑑別	使用預設密碼登入系統時，應於登入後要求立即變更。	使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。
識別與鑑別	身分驗證相關資訊不以明文傳輸。	身分驗證相關資訊於網路傳輸時，不可直接傳輸明文(如密碼原始字串)，避免被惡意攔截網路封包而外洩。
識別與鑑別	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該	系統應實作帳戶鎖定機制，於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。

	帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	
識別與鑑別	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，避免密碼被輕易破解。密碼最短效期可防止使用者為規避密碼歷程限制而於短期內頻繁變換密碼後又改回原始密碼。強制最長之效期之目的在避免固定使用同一組密碼。實務上，可參考政府組態基準(GovernmentConfiguration Baseline, GCB)之建議值，設定密碼複雜度及密碼使用效期限制。
識別與鑑別	密碼變更時，至少不可以與前3次使用過之密碼相同。	使用者前3次舊密碼應被保留(以雜湊值形式)，於設定新密碼時，比對新密碼與舊密碼之雜湊值，若雜湊值相同則拒絕此次密碼設定。
識別與鑑別	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	密碼重設機制設計不良可能造成安全問題，常見錯誤是系統自行產生隨機密碼後以電子郵件寄送給使用者，此問題在於無法確保傳輸過程經過加密保護，故提高資安風險。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，如電子郵件或手機號碼等，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性符記(如簡訊驗證碼、電子郵件驗證連結等)，一般會由亂數產生的英數字所組成，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳符記之有效性後，才允許使用者進行重設密碼動作。
事件日誌與可歸責性	訂定日誌之記錄時間週期及留存政策，並保留日誌至少6個月。	應依機關規定之時間週期及紀錄留存政策，保留系統事件日誌(Audit Logs)，目的包含程式除錯、行為歸責、稽核取證及法規要求等。
事件日誌與可歸責性	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	資通系統應實作記錄特定事件之功能，如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等。
事件日誌與可歸責性	應記錄資通系統管理者帳號所執行之各項功能	系統管理者為資通系統內具有最高權限之帳號，對系統及資料極具影響力，記錄所有管理者帳號執行之各項功能，有助於定期記錄系統行為及資安事件追查。

事件日誌與可歸責性	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。。	日誌應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。系統開發人員應盡可能採用單一的Log機制，如不得同時混用兩種以上日誌產生套件(如Log4Net與Nlog等)，並應確保日誌內容格式之可讀性，以便於事件比對與追查。日誌應依據資通安全政策及其他法規要求，納入任何有必要留存之資訊，如憑證資訊、日誌層級、會談識別碼等。
事件日誌與可歸責性	資通系統於日誌處理失效時，應採取適當之行動。	當資通系統發生日誌處理失效狀況時，應採取相對應的處理措施(如覆寫最舊的日誌紀錄、停止產生日誌紀錄或對特定人員提出警告等)，避免危害系統可用性，或是當資安事件發生時缺乏系統日誌以供比對追查之情況。
事件日誌與可歸責性	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	使用系統內部時鐘產生日誌所需時戳，如Windows作業系統顯示之日期時間等。採用全系統一致的時間標準，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。
事件日誌與可歸責性	系統內部時鐘應定期與基準時間源進行同步。	日誌紀錄必須維持使用精確的時間，以利事件追蹤及稽核取證等用途，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統及網路設備定期與校時伺服器進行同步，如國家標準時間伺服器(time.stdtime.gov.tw)或使用機關自建之伺服器。
事件日誌與可歸責性	對日誌之存取管理，僅限於有權限之使用者。	應施行日誌存取控管，避免未經授權使用者惡意讀取、竄改或刪除日誌紀錄。
事件日誌與可歸責性	依據日誌儲存需求，配置所需之儲存容量。	資通系統應配置日誌所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。