衛生福利部食品藥物管理署		
編號：3.供應	資訊委外共同說明書 (版本:4.7)	密等：普通
電子檔:中文 word.doc		頁次：第 1 頁共 35 頁

文件修訂變更履歷表			
版次	修訂理由及內容摘要	修訂頁次	核准日期
01	新制訂。		97.05.15
02	修訂2範圍、5.1、5.3、5.4、5.6、5.7、5.10、5.12、5.13、5.15、5.16、5.17、5.17.3、5.17.15、5.17.6、6、6.1、6.2、7	2-3	97.08.05
03	依據總統令「行政院衛生署食品藥物管理局組織法」，修訂相關程序	全部	99.01.01
04	依據100年外部稽核結果修訂相關程序	全部	100.08.16
1.0	1.依據文件管制規範重新修訂文件編碼 2.修訂5.3.3	全部	101.08.03 1012100015
2.0	101年執行結果檢討修正	全部	101.09.19 1012100143
2.1	修訂範圍貳二(八)3、系統基礎架構維護(十九)、二、委外廠商執行事項、(五)陸罰則二其他相關罰則	全部	101.09.27 1012100146
2.2	修訂範圍陸、罰則二、其他相關罰則(四)(五)(六)	全部	101.10.15 1012100161
2.3	修訂範圍壹四服務時限需求 (四)(六)、陸罰則一計罰方式 (一)、刪除陸一(四)	全部	101.10.16 1012100166
2.4	修訂範圍貳二(八)2差假規範刪除 (5)修正 (6)	P6	101.10.17 1012100168
2.5	修訂範圍參四(二)、伍二(五)、修正陸一(一)	全部	101.10.18 1012100170
2.6	修訂範圍叁三(二)、二(八)、(四)	全部	101.11.8 1012100193
2.7	修訂範圍貳二(八)1人員選任修正(5)新增(6)	P6	101.11.29 1012100237
2.8	修訂範圍壹三、貳二、貳三、參一二三四、伍二三、柒	全部	102.3.28 1022100057
3.0	新增流程圖修訂機關名稱及作業流程圖	全部	102.7.18 1022100165
3.1	修正壹四(一)及參二(一)；刪除原參一（三）21、原參四(十五)、肆二(二)及原	全部	102.8.27 1022150046

衛生福利部食品藥物管理署		
編號：3.供應	資訊委外共同說明書 (版本:4.7)	密等：普通
電子檔:中文 word.doc		頁次：第 2 頁共 35 頁

文件修訂變更履歷表			
版次	修訂理由及內容摘要	修訂頁次	核准日期
	伍三(一)； 新增原參一（三）22、參四(二十二) 及伍二(五)及其他文字修正		
3.2	修正伍二(二)1、陸二(一)、柒七及作業流程圖	P21、P24、P26	102.9.2 1022150051
3.3	依據國家資通安全會報 102 年 9 月函頒「國家資通安全通報應變作業綱要」新增參一(四)3 及陸二(七)，修正伍二(二)1、修正壹四(二)	P4、P12、P21、P24	102.10.09 1022150090
3.4	修訂部分文字、增列參、四、(二十三)、及引用罰則項目	P4- 6、P 8- 10、P 14、P 21、P 25	102.11.14 1022150154
3.5	依據行政院秘書長 102 年 6 月 12 日院臺護字第 1020137310 號函增列參、四、(二十四)	P14	102.11.25 1022150161
3.6	修訂參、四、(二十四)文字及柒、相關表格： 增列二十五	P14、P25	102.11.28 1022150177
3.7	新增陸、(罰則)二、(其他相關罰則)八	P25	103.02.26 1032100042
3.8	依據行政院 103 年 6 月 23 日院臺護字第 1030134245 號「國家資通安全通報應變作業綱要」新增壹三(一)；修正伍三(一)、陸二(一)(三)(七)、柒三四及捌	P3,P22,P24, P25,P27	103.07.09 1032100140
3.9	依據行政院國家資通安全會報推動政府組態基準設定及 103 年執行檢討，修正貳二(八)、伍一(一)、伍一(二)、伍一(三)2、伍二(一)、伍二(二)、伍三(二)、陸二(一)、柒三、七、十五、十八及捌；新增貳三(三)、伍二(二)2、伍三(二)1、柒二十六、二十七	P7~8, P18-25, P27-28	103.09.30 1032100198
4.0	1.依據 ISO27001 修正文件大類，原文件名稱「3.管理-資訊委外共同說明書」 2.依 GCB 組態要求修正	P7~15, P17, P20~24,P27~P30 撰擬：江文尉	104.06.16 1042100197
4.1	1.修正遠端連線存取相關規定	P29 撰擬：江文尉	104.09.16 1042100260
4.2	遵循行政院「資訊系統分級與資安防護基準作業規定」要求暨新增網頁 HTML5	p.8,p.14,p.16,p.28	105.03.25 1052100086

文件修訂變更履歷表

版次	修訂理由及內容摘要	修訂頁次	核准日期
	要求;「行政院資通安全會報技術服務中心」於 105.01.20 改制「行政法人資通安全科技中心，簡稱資安科技中心」	撰擬：江文尉	
4.3	1.行政院 105 年 8 月 8 日院臺護字第 1050172402 號函 8 月 1 日成立資安處。 2.修正資安及專案人員相關要求及雲端驗證選項	p.8,p.11~12,p.14, p.17,p.29~30 撰擬：江文尉	105.08.31 1052100207
4.4	修訂委外廠商須遵守事項與交付文件並調整災演文件驗證事項並依 106 年度外部稽核發現修正。	p.5,p.12,p.16,p.17,p.21, p.23p.25~26,p.27,p.31 撰擬：江文尉	106.8.29 1062100195
4.5	1.依據行政院相關政策，修正 GCB、ODF 規定。 2.修正災難復原演練規定。	p.16~17,p.25 撰擬：江文尉	107.8.3 1072100126
4.6	1.依據資通安全管理法及施行細則修正相關規定。 2.因應 107、108 年專案執行結果及事件檢討改進。	p.15,p.17,p.21,p.22,p.24 p.28,p.30~31 撰擬：江文尉	108.8.5 1082100113
4.7	依 108 年外部稽核發現檢討辦理。 1.廠商人員參與資訊安全教育訓練規定。 2.廠商稽核發現未改善之處罰。	p.29~30 撰擬：江文尉	108.8.23 1082100125

目錄

壹、前言 6
一、說明書圖例說明 6
二、 概述 6
三、適用性聲明 6
四、服務時限需求 7
貳、專案管理 8
一、專案執行計畫 8
二、廠商專案小組成員資格及工作內容 8
三、專案小組成員審核及更換 11
四、專案監控 11
參、建構管理 14
一、系統維護管理 14
二、系統變更及新增管理 15
三、保固責任 16
四、系統基礎架構維護 16
肆、文件及版本管制需求 18
一、文件製作範本 19
二、版本管制需求 23
伍、資訊安全 23
一、資訊安全政策說明 23
二、委外廠商執行事項 27
三、資安監控 30
陸、罰則 31
一、計罰方式 31
二、其他相關罰則 32
柒、相關表單 33
捌、作業流程圖 31

壹、 前言

一、說明書圖例說明

- ✧ 以“☐” 符號表示該項條文不適用
- ✧ 以“☑” 符號表示該項條文適用
- ✧ 無“☐”及“☑”符號表示該項條文適用
- ✧ 字元以紅色字體表示機關承辦人員需特別注意事項，如:「專案標的」
- ✧ 字元以網底表示廠商需特別注意事項，如：「會議中報告」
- ✧ 字元以黑色底線表示罰責說明，如：「違反本條任何所述者視同」

二、概述

本機關為配合政府資訊委外服務政策，將資訊服務委託民間辦理。為使本機關之委外專案能在符合資訊安全政策之前提下達成機關之目標，特訂定此說明書，以期本機關所有資訊委外專案具有良好且一致之服務水準；資訊委外專案須考量是否核心系統、是否涉及機密性或敏感性資料、系統是否對外部人員開放使用等，評估是否引用本說明書及調整適用條文。

三、適用性聲明

（一）資訊委外含概委託管理、委託建置及委託民間興建營運後轉移(Build-Operate-Transfer, BOT)之資通訊系統或關鍵資訊基礎設施。

（二）本文件屬於機關資訊委外之通用性規範，除需求說明書另有規定者外，適用本說明書。

（三）需求說明書優於資訊委外共同說明書內之其他文件所附記之條款。但附記之條款有特別聲明者，不在此限。

（四）各專案須就各系統之特性，於需求說明書或契約本文載明下列事項，以明確定義適用範圍。

1. 專案標的(計畫執行工作內容)
2. 履約期限
3. 現況說明(如程式大約總支數或程式清單)
4. 專案人員組成
5. 是否提供駐點人員或專線服務電話(5X8)
6. 新增及擴充需求

7. 教育訓練需求
8. 應交付文件
9. 未來每年維護費占建置費比例(適用資訊系統建置案)
10. 滿意度調查結果報告是否列為交付文件

（五）本說明書所列附表之格式及內容僅為參考範本，機關承辦人員得視實際需要進行修訂。

四、服務時限需求

（一）專案啟動會議：廠商須於**決標日次日**（如於108年決標，則自109年1月1日）起20個日曆天內召開。

（二）專案工作計畫書：**決標日次日**（如於108年決標，則自109年1月1日）起1個月內提交。

（三）□問題反映系統：使用者於問題反映系統反映之問題，廠商應於8工作小時內回應。

（四）□資訊系統維護服務單

1. □應用系統
   (1) 系統資料維護：7個日曆天完成。
   (2) 系統資料下載：7個日曆天完成。
   (3) 系統程式錯誤維護：7個日曆天完成。
   (4) 系統功能錯誤維護：7個日曆天完成。
   (5) 其他：依雙方議定時程辦理完成。
2. ☑硬體維護
   (1) A級硬體維護：
   A、機關日常運作中之系統所使用設備屬本案維護標的者，若故障導致系統無法正常運作時，廠商須於接獲通知後4小時(日曆天)內恢復設備正常運作(含OS安裝、列印及網路)。
   B、本案維護標的故障，惟所屬系統尚可運作(例如具有Redundancy or HA等機制)或非屬機關日常運作系統，廠商須於接獲通知後1個日曆天內恢復設備正常運作(含OS安裝及列印)。
   (2) B級硬體維護：機關通知廠商後，2個日曆天內恢復設備正常運

作(含 OS 安裝及列印)。

(3) 其他：機關通知廠商後，3 個日曆天內恢復設備正常運作。

(五) □系統變更及新增管理：於 1 個月內完成需求訪談及確認並於需求確認後 1 個月內完成(含測試完成)，系統開發步驟請參考『系統開發流程』。

(六) 契約中規範之事項，如未敘明完成時限，廠商以『資訊系統維護服務單』配合辦理。

(七) 上述規範，違反本條任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰。如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

貳、 專案管理

一、專案執行計畫

(一) 工作計畫管理

廠商須以書面方式提交『專案工作計畫書』，內容請參考「文件及版本管制需求」之「文件製作規範」，作為雙方運作之依據，並於『工作小組』會議中通過，違反本條任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

二、廠商專案小組成員資格及工作內容

(一) 專案經理 (專案負責人)

1. 須具有管理系統、協調整合專案實績經驗。
2. 具備專案經理、☑分析師、☑設計師相關經驗。
3. 掌握專案進行情形。
4. 負責管理駐點人員相關事宜。
5. 出席專案會議。
6. □通過機關需求說明書條文測驗及格。
7. 明瞭機關駐點人員會議紀錄內容，並負責督促執行會議決議事項。

（二）專案監控人員

1. 分析業務資料流之情形，並提供監視作業處理流程。
2. 監看資料流運作情形，並依機關要求提供報表。
3. 配合機關需求，至指定地點工作。

（三）□系統分析師

1、具備系統之需求分析與設計能力並具相關經驗。

2、須配合機關需求，至指定地點工作。

（四）□程式設計師暨資料庫管理師

1、負責開發程式及維護系統。

2、須配合機關需求，至指定地點工作。

（五）□資安技術師

1、國際電腦稽核師(CISA)證照或

2、國際資訊安全管理師（CISSP）證照或

3、認證道德駭客（CEH）證照。

（六）□管理顧問師

1、具備管理系統主任稽核員證照並具相關經驗。

2、ECSA Foundation 或 CSA CCSK 證照。

3、配合機關需求，至指定地點工作。

（七）□主管理顧問師

1、具備管理系統主任稽核員證照並具相關經驗。

2、稽核輔導實稽經驗 5 年以上擔任主管理顧問師。

3、ECSA Foundation 或 CSA CCSK 證照。

4、配合機關需求，至指定地點工作。

（八）文件及品質管理師

1. 開會及測試會議須到場。
2. 通過機關中文打字測驗，須達每分鐘 40 字以上。

（九）駐點人員

1. 人員選任

(1) □由廠商提供至少 5 倍候選名單，經機關工作小組覆篩通過。

(2) 試用期為 1 個月，若未通過試用，則需重新指派。違反本條任

何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先mail『工作小組』成員並經半數(含)以上成員同意。

(3) 須為大學畢業或曾於本機關服務表現良好者，薪資不可低於國科會專任助理薪資標準，機關得要求廠商於每季報驗資料中提供相關證明。

(4) □具備資訊安全或網路安全相關實務資歷。

(5) 駐點人員中斷期間，廠商須於 1 個月內依契約規範找到駐點人員，期間廠商應先行派人代理職務。

2. 差假規定

(1) 駐點期間為全天之工作時間，上班日依行政院人事行政總處公告為準；每日上班為 8 小時(不含午休時間) ；上班時間□9 時至 18 時或☑工作滿 8 小時(不含午休時間)或□依本署彈性上下班規範，上下班時須刷卡，代理人員亦同；如忘記刷卡或遲到每月不得超過 1 次。超過 1 次以上時，專案經理〈專案負責人〉了解其原因後提出說明，並自第 2 次起陪同駐點人員於駐點期間到場駐點，每超過 1 次陪同駐點 1 天。

(2) 遇履約標的發生異常之狀況，如可歸咎於廠商，須配合機關員工延長工時，機關不另計加班費用；如不可歸咎於廠商，機關得予加班補休，機關不另計加班費用。

(3) 駐點人員請假，需填寫『駐點人員請假單』，奉核後方可請假。如遇緊急情形，需事先口頭告知系統管理人員，且駐點人員請假單需後補。

(4) 駐點人員請假，廠商須另派人員代理職務；請假原因為病假或意外事故等不可抗拒之因素，廠商須於 2 小時內派人代理。

(5) 請假原因為加班補休或配合機關活動給予公假時，廠商不須派員代理職務，但需經機關系統管理員同意。

(6) 違反上述任何所述者，以陸、一、(一)、『未能於規定時間完成工作計罰』，如須延長日期或非廠商之問題(不納入計罰)，須經

『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

3. 工作內容

(1) 駐點人員須於機關指定日期、指定地點執行有關履約標的或機關指定之服務事項，其必要☑ OA 電腦或☑特殊工具軟體廠商須自行準備，並簽結『電腦使用申請表』、『軟體使用切結書』，且納入本機關資安相關規範管理。

(2) 駐點人員工作由機關駐點所在地職員安排及管理，如遇駐點人員無法依限期處理解決問題時，廠商應即增派人員支援。

4. 教育訓練

機關得要求廠商安排教育訓練計畫，以提升駐點人員專業能力，駐點人員應於工作小組會議進行心得報告。

三、專案小組成員審核及更換

（一）廠商應於本案『工作小組』會議中提出符合本案『專案小組』之人員，且須提出證明文件如勞保及公司證明文件、學歷及相關專長訓練證明文件，並提交『工作小組』會議同意後，負責處理與機關聯繫及執行本專案之事宜。

（二）廠商所指派之專案小組人員如須更換，應於『工作小組』會議同意後，始得更換；廠商之專案小組成員對於所應履約之工作有不適任之情形者，機關得經『工作小組』會議決議要求廠商更換，且廠商應於收到通知後 1 個月內更換，不得拒絕。

（三）廠商於專案期間內專案人員異動時，新進成員應簽立『保密同意書』及『保密切結書』，退離成員應對專案期間取得機關資料進行銷毀或移轉並簽立「專案期間取得資料銷毀/移轉切結書」。

（四）專案期間違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

四、專案監控

（一）機關為使專案順利進行且具一定之服務水準，依專案進行之需要，

得召開不同型式之會議，對專案進行監控，以期可順利達成專案之目的；工作小組之組成，由機關主導。

（二）會議種類

1. 專案啟動會議

廠商須召開「專案啟動會議」，報告專案之規劃。

2. ☑專案工作小組會議

(1) 廠商需於簽約後定期配合機關時程召開，原則上以每月為週期，頻率可由『工作小組』會議決議後調整。

(2) 會議之目的在檢驗本專案執行狀況，明定未確定之作業規範，解決發生之問題，討論雙方應配合及協調事項。

3. 技術討論會議

(1) ☑本專案進行期間，機關得視需要針對系統發生之問題要求廠商進行專題報告。

(2) ☑廠商需於得標後配合機關召開全部廠商技術討論會，討論共同議題。

4. 進度管控會議

本專案進行期間，專案進度落後或待解決事項非機關預期，機關得不定期召開進度管控會議，會議之目的在即時協商及盡速解決問題，使本專案執行狀況達專案計畫之要求。

（三）會議規範

1. 適用會議種類：專案啟動會議、專案工作小組會議

2. 會議前準備工作

(1) 廠商參加人員須包含①專案經理、②文件及品質管理師、③□駐點人員④□管理顧問師⑤□主管理顧問師及相關必要人員。

(2) ☑廠商須於會議前到場並完成相關環境及資料準備，並依『會議前準備文件檢查清單』所規範之內容完成會議準備，機關得視需要要求廠商提交『會議前準備文件檢查清單』供機關確認，如準備不及或延誤需事先告知。

(3) 會議前應將報告事項及文件經機關相關承辦人員或負責人完成確認，並更新至機關之版本管制平台。

(4) 專案期間違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

（四）會議進行規範

1. 會議紀錄人員，不得兼任專案報告人員(如：專案經理)且通過機關中文打字測驗。
2. 會議報告內容，機關得視管理需要增修內容。
3. 若廠商應報告內容準備不充份，會議主席得宣布散會，於廠商補齊資料後，再擇期召開。
4. ☑會議時必須進行錄音，錄音檔於會後 1 日(工作日)內上傳至本機關版本管制平台。
5. 專案期間違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

（五）其他

1. ☑廠商須於每次會議現場完成『會議紀錄』及大事紀要，同時請現場人員確認。並於會後 1 日(工作日)內以書面或傳真或電子郵件方式繳交及上傳至本機關版本管制平台。
2. ☑廠商須於每次會議準備 1 份檔案夾，放置相關歷次會議及合約書等資料，以利會議進行。
3. 會議決議如屬維護/變更需求，廠商應填寫『資訊系統維護服務單』/『應用系統變更申請紀錄表』後，由機關系統管理人員確認後辦理。
4. 廠商專案經理及駐點人員，應參加本署不定期舉辦之有關「契約」及「資訊委外共同說明書」之測驗，以驗證對相關內容有足夠之認識。
5. 廠商專案人員，應參加本署不定期舉辦之有關本署網路及資料庫等基礎架構之測驗，以驗證對相關內容有足夠之認識。

6. 專案期間違反上述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

參、 建構管理

一、系統維護管理

（一）□問題反映系統管理

1. 使用者使用系統遭遇問題時，可透過使用者問題反映系統反映，廠商接獲系統通知後，應於時限內回應。
2. 回應內容應包括下列項目：
   (1) 說明問題可能發生原因及種類。
   (2) 提出問題解決方式或替代方案；替代方案不得增加機關額外人力或資源。
   (3) 評估處理問題所需時間或完成期限。
3. 若使用者反映之問題涉及資料或程式異動時，廠商應填寫『資訊系統維護服務單』後，經機關系統管理人員確認後辦理。

（二）資訊系統維護服務單

當系統（含正式及測試環境）有下列之維護需求時，得由使用者/資訊室填寫本單，交由廠商進行維護工作：

1. 系統資料維護(系統無提供維護介面)；若因程式不正常之運作造成資料錯誤，由資訊室/使用者填寫『資訊系統維護服務單』經業務單位確認修正內容後修正。
2. 系統資料下載(系統無提供下載介面)。
3. 系統程式錯誤維護(如:出現錯誤訊息視窗)。
4. 系統功能錯誤維護(如:未出現錯誤訊息視窗，但程式之運作結果，未達原系統設計之預期)。

（三）技術諮詢及服務工作

1. 資料之傳輸、管理及整合之維護。
2. 系統功能之維護。
3. 緊急或異常狀況(包含當機及復原)處理。

4. 系統更新或擴充之技術支援。
5. 系統安全性之管理支援(如：系統使用紀錄及權限管制等措施)。
6. 系統問題排除。
7. 系統相關環境(作業系統及硬體)之問題追蹤。
8. 系統瑕疵與錯誤之修正。
9. 系統執行效能之調校。
10. 系統資訊安全弱點之修補。
11. 利用本機關提供之資安原始碼掃描工具進行系統原始碼弱點掃描並修補發現之弱點。
12. 系統災難復原文件之製作及維護與系統災難復原演練。
13. 系統相關軟體環境之安裝與設定。
14. 系統操作與管理之技術諮詢。
15. 檢修並排除系統日誌中所警示之錯誤。
16. 協助排除作業系統事件檢視器之「系統」錯誤事件。
17. 系統文件之修訂。
18. 配合出席機關召開之系統介接或技術討論會議。
19. 依機關要求提交系統維護服務紀錄。
20. 廠商須提出提升教育訓練參與人數及問卷回收率之方案並執行，所需人力與費用，概由廠商負責。
21. 每月定期進行系統檢測與暫存資料清理。
22. 配合機關要求，相關檔案上傳至機關版本管制平台。

（四）系統監控

1、提供機關所需自動監控機制(Host Monitor)之監控規則，以提升系統穩定性。

2、處理系統監控(Host monitor)事件之分析、釐清及處理等事宜。

3、資安監控(Security Operation Center, SOC)服務，應配合監控情蒐回傳機制，定期提供予技術服務中心。

（五）非保固期間之維護工作，應包含保固責任所規範之內容。

二、系統變更及新增管理

（一）□維護期間允許 6 %(以總程式支數估算)之彈性新增且現有程式變

更 3 支視為新增程式 1 支計算；廠商以『應用系統變更申請紀錄表』配合辦理，並依雙方議定時程辦理完成。

（二）程式完成修正上版至正式機前，廠商須與系統管理者即時聯繫，使機關充分掌握狀況。

三、□保固責任

（一）保固期間廠商需無償負責本章節所規範之事項。

（二）配合機關環境異動，如系統移機及環境重建等。

（三）提供技術轉移服務並修訂系統相關文件。

（四）定期弱點掃描(含作業系統、網頁及原始碼)，並修正高風險弱點直到確認已無不可接受之風險弱點。

（五）配合系統相關會議之召開。

（六）釐清系統相關問題並修正系統功能錯誤。

（七）依資訊系統維護服務單處理並回覆系統使用者相關問題。

（八）□處理問題反映系統相關問題。

（九）機關通知後，仍不履行上述條款，機關得逕行處理，所需費用，得自廠商保固保證金扣除。

四、□系統基礎架構維護

本章節係為促進機關整體基礎建設之推展，規範廠商通用性應配合項目，故需配合機關整體環境及個別系統之特性，以使用單位實際需求訪談及工作小組會議決議為原則，廠商以『資訊系統維護服務單』配合辦理，並依雙方議定時程辦理完成。

（一）□廠商負責建置測試機，並置原始碼及提供開發環境，且可編譯成執行碼，供機關資安原始碼掃描工具掃描。

（二）□提供系統簡介之單張資料，內容須清楚描述系統概念、目的及架構等，並加裱框，尺寸大小由本機關規定。

（三）□有關登入方式及權限管理，廠商須提供完整原始碼，作為資安驗證。

（四）□Server 端程式錯誤之錯誤訊息須寫至事件檢視器。

（五）提供各項非客製化軟體之使用授權及操作手冊等文件；非客製化軟體須提供最新版本。

（六）□配合現有 MS-SQL 資料庫整合，移至機關指定之資料庫，環境為 MS-SQL 2016 以上(版權由機關提供)。

（七）□配合內部系統 DB Table 介接需求，提供來源資料庫 Table 或 View。

（八）□配合現有資料庫於所有欄位註記中文使用說明。

（九）資料庫資料表格關聯需建立外來鍵，不得使用程式控制為原則。

（十）配合系統移機作業將系統移至機關指定之環境。

（十一）□廠商需修改帳號登入程式及帳號申請流程，以配合機關 Portal 單一簽入。

（十二）□系統目前介接如屬機關內部系統介接須使用 DB Table 介接方式，廠商需負責至來源資料庫中擷取資料；機關外介接使用 BizTalk 作為介接平台，廠商需負責維護介接資料庫之資料。

（十三）□配合資料異動之重要資料庫表格(Table)皆須紀錄最後異動之時間(last modify date)及異動者(等 9 個基本欄位)之程式修改，詳『Table 增加 9 個欄位』(如相關表單)；需求範圍依專案工作小組會議決定。

（十四）配合機關防火牆環境調整，作相對應設定。

（十五）□提供網址列之圖檔(favicon.ico)。

（十六）□須確保網站失效連結及無效檔案完全清除。

（十七）□配合機關資訊整合之「跨系統藥廠代碼整合方案」，系統作相對設定及調整。

（十八）配合機關升級 IPv6 協定，系統作相對設定及調整。

（十九）於伺服器端不需安裝 office 軟體，即可產生 office 文件。

（二十）配合機關 office 及 IE 環境升級，系統作相對調整。

（二十一）□廠商原則上不得使用 ActiveX 元件，如需使用必須經工作小組同意，且該 ActiveX 元件須經第三方公正單位驗證，所衍生費用由廠商支付。

（二十二）系統登入驗證如未整合本署 AD 帳號，則使用者密碼之長度、複雜度及更新期限，須依政府組態基準(Government Configuration Baseline，GCB)規範。

（二十三）☑依循政府組態基準(GCB)規範，本機關資通訊終端設備(如:個人電腦)於套用 GCB 一致性的安全設定後，系統須維持正常運作，

如未能配合，需經機關專案工作小組同意後，填寫『GCB 例外原則申請單』備查。

（二十四）☑依系統安全等級，資訊系統防護措施符合「資通安全責任等級分級辦法」附表十「資通系統防護基準」要求。

（二十五）□系統或網頁對不特定對象(如對民眾)開放時，優先以 HTML5 技術開發處理。

（二十六）□對外開放網站首頁應標示機關資訊安全政策及隱私權保護宣告。

（二十七）□對外開放網站若有提供可編輯文件供民眾下載時，應同時提供 ODF(Open Document Format 開放文件格式)文件。

（二十八）□特權帳號應具備雙因素(two-factor authentication)認證機制。

（二十九）□為確保開發之平台具備雲端特性，廠商建置之雲端平台應依據驗證時最新公告之「IaaS 服務雲端特性驗測作業程序」檢測項目，通過經濟部「雲端開發測試平台」（Cloud Open Lab）（http://www.cloudopenlab.org.tw）所建立雲端特性測試技術之驗證；驗證衍生之相關費用由廠商自行與驗證單位結算。

（三十）☑廠商應定期(每年至少 1 次)清理舊資料，應清理之資料與頻率於工作小組會議決議，決議後廠商未執行依「未依會議決議執行」辦理。

（三十一）系統因故未採用 gMSA 帳號者，若未依規定定期變更 AD 帳號密碼而導致系統無法正常運作，每次計罰 1 點。

（三十二）系統應每至少 500 日曆天重新啟動一次，未依規定重新啟動，每次計罰 1 點。

（三十三）□廠商為客製化資通系統開發者，應提供該資通系統之安全性檢測證明。

（三十四）□非廠商自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

肆、 文件及版本管制需求

下列文件項目僅供參考，廠商以能符合機關了解本專案實際運作、維護為基本原則。

一、文件製作範本

（一）專案工作計畫書

專案工作計畫書應包含下列事項：

1. 人力配置：維護系統之專案人員之人力配置。
2. 工作計畫項目(包含契約所有重要需求)。
3. 資訊安全管理計畫。。
4. 個資適當安全維護計畫。
5. 災難復原管理。
6. □通過機關需求說明書條文測驗及格證明。

（二）需求規格書

需求規格書應提供使用者角度的需求陳述且應包含下列事項：

1. 系統建置之目的
2. 需求示意圖(需描述使用對象及主要業務功能)
3. 業務功能描述(說明各項功能目的、資料來源及資料輸入者)
4. 權限及管理需求
5. 名詞定義

（三）系統分析及設計規格書

1. 系統分析規格
   (1) 系統簡介：簡述系統之目的、功能、效益及結構等。
   (2) 系統功能定義：敘述主要功能及設計架構。
   (3) 系統介面及作業流程：說明本系統與其他應用系統之關連，及有關之作業程序。
   (4) 服務系統安全與控制：說明服務系統作業安全上應有之控制措施。
   (5) 物件關聯圖及說明：說明服務系統各物件間之關聯。
   (6) 共用模組(含概述及功能)。
2. 程式設計規格
   (1) 程式概論：包括依據／目的、程式概述、修正紀錄及輸出入檔案關聯圖。
   (2) 程式設計說明：包括程式設計要點及程式模組結構。
   (3) 處理程序：包括批次程序說明及線上操作說明。

3. 程式設計之細部設計說明

撰寫格式參照『程式設計之細部設計說明』，內容應包含下列項目：

(1) 螢幕/報表畫面。

(2) 使用之程式名稱說明。

(3) 使用時機及流程。

(4) 起始動作說明

(5) 欄位說明

A、使用時機。

B、欄位初始說明。

C、相關代碼/編碼說明。

D、檢核條件。

E、計算說明。

(6) 程式邏輯/產生邏輯。

(7) 相關資料表及資料庫。

(8) 動作(Button/Link)說明。

A、寫入之相關資料庫。

B、寫入檔案。

C、相關動作。

(9) 修正歷程及會議決議說明

4. 資料庫之資料庫綱要及實體關係資料模型(E-R Model)

本需求欄位總表主要是把主題計畫的需求經系統化，並列成表單供系統開發人員建置資料庫時設定欄位所用，同時也供程式設計人員在撰寫程式時參考使用。需求欄位說明如下：

(1) 資料表綱要

A、 項目名稱：所需著錄項目之中文名稱。

B、 英文名稱：項目名稱對應之英文名稱。

C、 資料型態：資料之資料型態。

D、 大小：欄位所需之空間。

E、 必填：標示“＊”者表示為必填欄位，建檔時須填寫該欄位

之值，不能空白。

F、 多值：標示“◎”者表示為多值欄位，該組欄位資料可重覆著錄。

G、 屬性：標示該欄位的屬性，包括：

(A) 「唯一」表示欄位的值在資料庫中是唯一存在的。

(B) 「不開放」表示該欄位只供管理者使用，不對外開放。

(C) 「下拉式選單」表示記錄方式為下拉式的選單。

(D) 「系統自動產生」表示該欄位的值是由系統自動產生，非由著錄人員著錄。

H、 提供者：記錄這筆資料是由系統自動產生或由填表人所填入。

I、 備註(欄位檢核邏輯，如：必填、選填、不可填之關係及可作為註記上述未考慮之說明，如資料格式或限制)

(2) 欄位代碼表

5. 作業處理流程 Process flows

(1) 各項業務處理作業。

(2) 帳號申請/刪除處理作業。

(3) 密碼修改處理作業。

(4) 系統備份處理作業。

(5) 系統安裝處理作業。

(6) 系統事件處理作業。

(7) 系統維護處理作業。

(8) 系統轉介接處理作業。

(9) 其他處理作業。

（四）系統管理手冊

1. 系統簡介：包括系統之目的、功能及結構等。

2. 服務系統操作目錄說明：說明主要目錄(Menu)之各項功能說明。

3. 服務系統作業程序：包括各項定期作業，報表列印等各功能執行程序之參數維護、訊息顯示等作業流程及說明。

4. 服務系統維護須知:說明執行服務系統日常維護工作應注意事項，

例如上下系統程序、經常性作業程序、系統意外事故處理程序、系統故障之分析與排除等。

5. 訊息說明與處理。

（五）系統操作手冊

1. 服務系統簡介：包括服務系統之目的、功能及結構等。
2. 服務系統編碼說明。
3. 輸入表單說明：說明須使用之表單格式及其輸入欄位之引用方式。
4. 服務系統作業說明：包括每日、月底、季末、年底等參考(標準)檔維護、系統資料維護等作業流程及說明；線上作業並應說明其使用時機。
5. 服務系統操作說明：服務系統基本操作方式，各線上及批次功能使用方法，螢幕範例，報表列印及檔案維護方法等。
6. 報表列印。
7. 錯誤訊息說明與處理。

（六）系統安裝手冊(廠商依實際需求製作)

（七）災難復原手冊(廠商依實際需求製作)

（八）系統壓力測試報告

1. 說明使用之壓力測試工具、測試之軟硬體環境。
2. 依據測試數據提供下列結論：

(1) 目前正式環境及常態使用下之平均回應時間。

(2) 目前正式環境中最大使用者數與平均回應時間。

(3) 增加硬體資源後之最大使用者數與平均回應時間。

(4) 所需硬體環境由機關提供。

（九）系統測試報告書

檢附單元(或整合)測試報告，其中須逐項敘明包括測試期間、測試項目、測試條件(或資料)、測試畫面、發現之問題數、與測試者簽名等。

（十）系統功能需求確認報告書，需經機關需求使用者確認。

（十一）滿意度調查結果報告(廠商依實際需求製作)

1. 已填答的問卷。
2. 彙整及回應問卷中反映的文字意見。

二、版本管制需求

□原始碼需置於本機關版本管制平台，□並於機關測試機/開發機編譯後，再將其更新至正式機。

伍、 資訊安全

一、資訊安全政策說明

（一）廠商能力要求與工作說明

1.廠商辦理業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

2.廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

3.廠商辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

4.依據資通安全法施行細則第 4 條第 2 項，委託業務涉及國家機密(國家機密指已依國家機密保護法核定機密等級者)之專案，廠商執行本專案且可能接觸國家機密之人員，應接受適任性查核，並依國家機密保護法之規定，管制出境。得標廠商亦須提出參與業務執行人員之國籍者說明，於下列選項勾選人員安全管控需求：

□屬經濟部投資審議委員會公告『具敏感性或國安(含資安)疑慮之業務範疇』，或涉及國家機密，禁止來自大陸地區、第三地區含陸資成分廠商或在臺陸資廠商；得標廠商之專案成員中不得有具大陸地區或香港、澳門身分，或曾於該等地區擔任其黨務、軍事、行政或具政治性機關(構)、團體之職務，其分包廠商及其專案成員亦同。

□屬具敏感性或國安(含資安)疑慮之業務，或涉及國家機密，廠商執行本案業務之專案相關人員如具中華民國以外之國籍，須於投標時敘明之。

5.廠商提供服務，違反資通安全相關法令或知悉資通安全事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。

（二）委外廠商及人員管理

委外廠商及其專案人員應確實遵守機關之資訊安全政策，且廠商及其專案人員應簽署『資訊業務委外廠商資訊安全聲明書』、『保密同意書』、『同意不將專案移至境外執行聲明書』、『保密切結書』；廠商駐機關人員需另檢附『軟體使用切結書』，必要時機關並得檢視其身分證明文件。

（三）□系統開發設計及變更維護管理

1. □機敏資料處理程序

以下所稱機敏資料係指機關持有或保管之資訊，依國家機密保護法、個人資料保護法等相關法規及機關實際需求訂定者；廠商以『資訊系統維護服務單』配合辦理，並依雙方議定時程辦理完成。

2. 加解密

(1) □密等以上資料不得電子傳輸，如有傳輸需求應向專管單位申請加密機制專門使用，敏感資料在傳輸過程中應加密保護(如□TLS1.0、□TLS 1.1、☑TLS 1.2 等)以確保其機密性。

(2) □敏感資料儲存時，需使用加密技術或其他適當措施，確保其機密性。

(3) □廠商應遵循機關訂定之資料保密規範或國際認可的加密技術(如 AES、3DES、Blowfish 等)，以確保符合安全要求。

(4) □敏感資料下載檔案須加密後才可下載。

(5) □系統採行加密編譯，廠商需符合 FIPS 140 規範之加密演算法，包括加密、雜湊以及簽署演算法。

3. □存取控制

(1) □敏感資料存取，系統或架構設計需可限制特定使用者 IP。

(2) □敏感資料下載或查詢等，使用者界面需顯示資安警語。

(3) □一般使用者查詢(含列印)敏感資料者時，個人資料(姓名、身分證統一編號、生日、居住地址、私人電話)不得顯示足以識別該個人，如：身分證統一編號後 4 碼（即第 7 碼至第 10 碼）進行遮蓋，並以「*」取代，如另有特殊性用途則依相關規定辦理。

(4) □敏感資料使用者列印或查詢客製化報表，其輸出需產生註記(使用者姓名、日期、時間等)，必要時機關得要求查詢介面提

供驗證碼功能。

4. □功能測試：於測試機進行測試作業時，不得以正式資料、敏感資料進行測試。

5. 通行碼(密碼)管理

(1) 新增、修改通行碼時需驗證下列規則：通行碼長度應為 12 碼(含)以上，且包含英文大寫、小寫、數字、特殊符號(4 選 3)等。

(2) 系統應提供更新通行碼機制，包括期限參數設定、逾期鎖定、到期提示等。

(3) 通行碼輸入錯誤 5 次，需鎖定帳號。或採用驗證碼機制：帳號登錄頁面與新申請頁面都有驗證碼欄位供使用者輸入。

6. □帳號管理

(1) 系統應依使用者權限提供系統帳號及權限查詢介面。

(2) □使用者帳號避免以身分證統一編號為帳號。

(3) □特殊情況需以身分證統一編號為帳號者，應以「*」取代方式處理後使用，同時需考慮相關延伸應用。

(4) □應於伺服器端採行集中過濾檢查使用者之權限作業。

7. □輸入資料確認

為防止 SQL Injection 等漏洞造成資訊系統中的輸入資訊錯誤、遺失與未經授權的修改或使用，系統中所有輸入欄位應進行資料格式、長度等檢查。

8. 系統日誌

(1) 需提供系統稽核軌跡(Log)，留存使用者帳號☑新增、☑異動、☑刪除記錄。

(2) ☑留存篩選資料之新增、異動、刪除記錄，必要時留存 SQL 指令。

(3) ☑採用單一日誌記錄機制，確保輸出格式一致性，且記錄必要的使用者資訊及管理者行為，排除敏感資訊。

9. ☑防駭及弱點掃描

(1) ☑檢查並確認作業系統、資料庫系統及相關套裝軟體是否已安裝最新修補檔，或關閉有漏洞服務，以減少有心人士利用已公布

的系統弱點而產生的風險。

(2) □應用系統須通過資安原始碼掃描工具掃描及網頁弱點掃描工具(如 IBM APPSCAN)之驗證，若掃描結果有不可接受之風險弱點，則廠商需於系統弱點修補後，限期內申請復檢，廠商並應追蹤檢討直到確認已無不可接受之風險弱點。

(3) 以防毒及防駭軟體掃描應用系統程式，以確認程式中是否存在已知的木馬或後門程式。

(4) 檢查測試應用系統與資料庫連線是否正常 (資料庫與應用程式間之連結須設定,不可把資料庫存取權限開放給非應用程式主機來連線，原則上只限開放給應用程式連結資料庫)。

(5) 應用系統安裝其執行權限原則上不得使用 Administrator、sa、root 等管理群組執行。

(6) 進行遠端存取功能測試，測試是否關閉不必要的遠端存取功能等；遠端存取如屬必要，須填寫『遠端連線服務申請表』及『遠端連線存取使用紀錄表及動態密碼異動紀錄』；嚴禁廠商私設遠端維護機制，以杜絕網軍入侵管道，違反則採以陸、二、(一)、資安事故 2 級以上罰則。

(7) 網頁根目錄放置 robots.txt，虛擬目錄進行安全設定且應移除範例、預設目錄且不可使用預設值。

(8) 交付軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

（四）□日常作業

1. □程式原始碼管控

(1) □原始碼及編譯程式禁止置於正式作業環境之作業系統內。

(2) □應建立原始碼程式庫的更新活動稽核日誌。

(3) □程式換版應提供修改變更比較表，並提供測試記錄，經機關人員審核後，才能換版，舊版程式原始碼需至少保留 3 代，以作為程式緊急回復措施之用。

2. 系統文件管理

(1) 系統相關文件(如：系統之操作手冊)應詳述資訊安全控制措施(如：備份與回復方式)，俾使使用者及技術支援人員瞭解系統之安全控制措施。

(2) 需提供『災難復原手冊』文件。

二、委外廠商執行事項

（一）☑弱點掃描

1. ☑作業系統弱點掃描

系統運作之相關主機，須通過作業系統弱點掃描工具之驗證，若掃描結果有不可接受之風險弱點，則需於系統弱點修補後，申請復檢，直到確認已無不可接受之風險弱點，廠商以『弱點掃描申請暨修補處理單』提出申請，至少每季(季末 15 日前)一次。

2. □網頁弱點掃描

應用系統須通過網頁弱點掃描工具(如 IBM APPSCAN)之驗證，若掃描結果有不可接受之風險弱點，則需於系統弱點修補後，申請復檢，直到確認已無不可接受之風險弱點，廠商以『弱點掃描申請暨修補處理單』提出申請，至少每季(季末 15 日前)一次。

3. □程式原始碼掃描

應用系統須通過資安原始碼掃描工具，掃瞄系統所有程式，直到確認已無不可接受之風險弱點，掃瞄報告併同於該季報驗，廠商以『程式碼安全弱點掃描申請單』提出申請，至少每季(季末 15 日前)一次。

4. 違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

（二）☑災難復原

1. 災難復原演練

(1) 廠商須每年定期進行災難復原演練，情境由機關指定之，並依『災難復原演練計畫』及『災難復原手冊』完成演練詳實記載於『災難復原演練紀錄』，且依據演練結果調整『災難復原演

練計畫』及『災難復原手冊』。

(2) □廠商於演練完成後次日起 7 天內進行資訊系統切換至正式營運區驗證復原有效性。

(3) 演練前，系統負責人應依據演練準備清單完成檢查，演練當日若查檢表顯示尚有缺漏，即取消演練，由系統負責人另擇期提出申請。

(4) 演練當日，由本署現場抽選廠商專案成員中任 1 人進行演練，若無法全員到場，則廠商須於所排定演練日之 1 週前提供演練相關文件，由資訊室指定人員，代為驗證文件完整性與執行時間；人員須於時限內，依據演練計畫執行步驟完成復原演練標的建立，且功能驗測無誤，方視為演練文件有效。

(5) 資訊安全管理系統輔導廠商未能明確檢核相關文件及提供改善建議，視為資安輔導廠商違反規定。

(6) 違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

2. 『災難復原演練計畫』及『災難復原手冊』文件正確性驗證

(1) ☑廠商應提供正確災害復原手冊，且確實維持完整性，每年文件正確性應定期驗證(每年至少 1 次)，由機關指定人員排定驗證時程並經核准後執行。

(2) ☑廠商須於機關排定確認日期前完成更新合約範圍內的『災難復原演練計畫』及『災難復原手冊』，其內容須符合合約要求時限。

(3) ☑由機關指定人員依『災難復原手冊』進行確認，並詳實記載演練過程，驗證文件正確性。

(4) 若機關指定人員依廠商提供之『災難復原演練計畫』及『災難復原手冊』操作步驟無法完成文件正確性驗證作業，

☑廠商須證明是否為機關指定人員操作錯誤，否則視為廠商違

反規定。

☑若經證明機關指定人員操作錯誤,於資訊室會議中報告錯誤原因。

☑若經證明為資訊安全管理系統輔導廠商未能明確檢核相關文件及提供改善建議，視為資安輔導廠商違反規定。

(5) 違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰,如須延長日期或非廠商之問題(不納入計罰),須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

3. 系統故障無法運作之修復

(1) □應用系統：因系統故障無法運作時，如為本案範圍，廠商須於接獲通知後 4 小時(日曆天)內到場處理，並於 1 個日曆天修復完畢。

(2) ☑硬體維護：同 A 級硬體維護之服務時限需求。

(3) 專案期間違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰),須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

(三) ☑參與資訊安全教育訓練

1. 配合機關資訊安全政策，本專案全職及非全職人員均須配合機關要求，參加機關規定之資訊安全教育訓練及資安會議。
2. 廠商本專案人員應比照本署人員每年應參與資訊安全教育訓練，依「資通安全責任等級分級辦法」規定，技術人員(如專案經理、系統分析師、程式設計師、資料庫管理師及其他技術相關職務)每人每年應接受三小時以上之資通安全專業課程訓練，其餘人員每人每年應接受三小時以上之一般資通安全教育訓練；機關得要求廠商出具人員參與訓練證明(本署資訊安全教育訓練或外部資訊安全教育課程)，廠商若無法提出證明，每人次計罰一點。

(四) ☑提供系統資訊安全風險評鑑相關文件及資訊資產清冊

廠商需提供系統資訊安全風險評鑑相關記錄文件及資訊資產清冊等建議文件。

（五）廠商應配合提供符合「資通安全責任等級分級辦法」附表十資通系統防護基準要求之資通安全相關紀錄。

三、☑資安監控

（一）☑委外廠商稽核查檢

1. 委託機關應定期或於知悉廠商發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。
2. 廠商需提供其內部資安控管之稽核項目供機關參考，可參考『委外廠商稽核評估表』，機關得依廠商委外作業之各項資安風險等級進行評估後，不定期依相關稽核評估內容進行抽核。
3. 廠商應確實改善稽核查檢發現之缺失，若稽核查檢仍發現前次稽核發現之相同缺失未改善，每一缺失計罰一點。

（二）☑敏感資料及個人資料維護

1. 廠商需對機關提供之業務或個人資料，包含紙本文件、電子檔案及電子郵件信箱附加檔案等任何形式存在之業務或個人資料應加以保護不得洩漏。
2. 廠商如需將專案複委託時，須事先獲得機關同意，且廠商應要求複委託廠商遵守本規範。
3. 機關正式環境之資料嚴禁廠商攜出，若需測試資料，須經特別處理以去除其機敏性。
4. 廠商於合約終止或解除前一個月，提出受委託期間曾接受機關交付之業務或個人資料盤點清冊，其內容應包括交付各種紙本及載體。並於合約終止或解除時，提交具體指明相關資料銷毀、交還機關或交給機關指定之另一個機關之證明，內容包括銷毀或交還之項目、數量、時間、方式、簽收人等，並交付切結文件「合約終止資料處理聲明」證明未持有機關之所有交付之資料。如因故未能銷毀、交還或交給機關指定之另一個機關，應列冊載明原因及保存的期間、方式，於取得機關之同意後進行保存。
5. 廠商對於個人資料保護需記錄下列各項執行結果，並定期提供機

關相關紀錄：

(1) 廠商應確保專案成員明瞭專案可能涉及個人資料之蒐集、處理及利用之範圍、類別、特定目的及期間，並承諾僅就機關指示範圍內蒐集、處理及利用個人資料。

(2) 廠商執行個人資料蒐集、處理、利用之結果，其中包括蒐集、處理、利用個人資料數量、方式、範圍、時間以及是否符合機關特定目的等內容，相關表單可評估加註標示：「**本資料因涉個人資料，請依法妥善蒐集、處理、利用及保管**」。

(3) 廠商應遵守機關所訂定之資訊安全相關規範、及個人資料保護法所要求採取之適當安全維護措施，並建立個資管理流程及做好防止使用者個人資料外洩之安全控制措施。廠商應定期繳交已實施個資法訂定適當安全維護措施之證明文件(如內外部稽核結果等)。

(4) 廠商或其員工違反個人資料保護法、其他個人資料保護法律，或其他法規命令時，應通知機關違法之事實及欲採行之補救措施，並依個人資料保護法第 12 條之要求通知當事人及負個人資料保護法相關損害賠償責任。

(5) 廠商應遵守專案要求相關保留指示事項，並回報其遵循結果。

陸、 罰則

一、計罰方式

（一）未能於規定時間完成工作計罰

以日曆天計罰，計罰違約金不足 1 日以 1 日計，每日計罰 1 點；未能於規定時間完成工作計罰之計算，為自機關通知(書面、傳真、系統報修或電子郵件)之發生時間(工作時間)起算，至功能恢復正常運作且經機關人員確認止(日曆天之計算不含前 2 次機關人員測試時間，第 3 次起含機關計算測試時間，計算方式詳如『未依規定時間完成工作計罰天數之計算說明表』；契約中不含機關測試部分，依契約規定時間完成)。

（二）重覆報修定義

當案件發生多次報修，且經工作小組認定其原因相同，則罰款以最

早發生日期為起算點，並以最後結案時間為結算點。

（三）上述違約金依原因每件(申請單)獨立計罰，罰款天數以日曆天計。

（四）本案標的物如逾維修期限未修護或執行完成，且廠商無法提出令機關同意之延遲原因時，機關得另行招商修護，修護相關費用概由廠商負擔及賠償。

（五）本案功能新增修改部份仍受維護條款規範。

（六）凡在保固期內發現瑕疵，應由廠商於機關指定之期限內負責免費無條件改正。逾期不為改正者，機關得逕為處理，所需費用由廠商負擔，或動用保固保證金逕為處理，不足時向廠商追償。但屬故意破壞、不當使用或正常零附件損耗者，不在此限。

（七）本案每點違約金金額依契約規定，若契約未規定訂為每點新臺幣 3 仟元整。

二、其他相關罰則

（一）廠商應做好資通安全與防止個人資料外洩之相關配套措施。專案執行及保固期間，發生資安事件 2 級含以上、個資外洩事件或其他因素而造成機關不名譽事件等，且可歸責廠商者，每次予以本專案得標總金額 5%懲罰性罰款，除限期改善外，並由承包廠商負責處理並承擔一切法律及賠償責任；機關發生資安事件 1 級含以下並經行政院國家資通安全會報技術服務中心發送事件通知或發生白帽駭客事件，且可歸責廠商者，每次予以懲罰性罰款 3 仟元整。

（二）系統修改或新增需以『應用系統變更申請紀錄表』為依據，系統資料維護或下載需以『資訊系統維護服務單』為依據，如未經相關表單程序核可或資訊系統負責人或資訊系統管理人同意即異動系統程式、功能、資料，每次予以本專案得標總金額千分之 3 懲罰性罰款，惟以上罰款，最高上限 3 仟元整。

（三）廠商收到機關開立『資訊安全異常處理單』，應立即判定資安等級並進行異常原因調查分析，未於 1 個月內提出具體原因及改善措施，屆時，每次予以懲罰性罰款 1 仟元整。

（四）因系統功能發生異常機關開立『資訊系統維護服務單』，廠商如無法找出原因，每次記 1 點，超過 3 點(不含 3 點)以上每增加 1 點懲罰性

罰款 3 仟元整或☑硬體廠商可以更換整台硬體設施代替罰則。

（五）系統當機須重新開機或服務重啟，廠商如無法證明非系統問題，每次記 1 點(機關以書面、傳真、系統報修或電子郵件紀錄)，超過 12 點(不含 12 點)以上每增加 1 點懲罰性罰款 3 仟元整。

（六）廠商如需遠端管理系統須填寫『遠端連線服務申請表』申請遠端連線，並於規定時間內辦理展期(每年 6 月及 12 月)、盤點及交付(每月 10 日前)『遠端連線存取使用紀錄表』，如違反上述規定，每逾 1 日予以懲罰性罰款 1 仟元整；每月交付之『遠端連線存取使用紀錄表』

□漏列連線次數(閒置時間三十分鐘內可列同一次)或時間區間超過 30 分鐘(含) 等內容未確實填寫，若當年度累計達 3 次(以月為單位)將予以懲罰性罰款 3 仟元整；並累罰(以星期為單位)至改善為止。

□內容未確實填寫，經系統管理者判定情節重大者，將予以懲罰性罰款 6 仟元整；並累罰至改善為止(以星期為單位)。

☑內容未確實填寫，將予以停用，改善完畢後至工作小組會議報告。

（七）廠商未依「**資安事件通報應變作業規範**」落實資安事件通報應變作業及提供資安紀錄等，致國家或社會受有重大損害時，將建議解除合約或依約罰款或不予續約；已遵循「**資安事件通報應變作業規範**」確實辦理資安事件通報及應變作業並提供資安紀錄，仍致機關或民眾權益受損時，機關得參酌減輕其責。

（八）除機關同意外，廠商原則上需每周(得配合專案需求變更頻率及時間)就所維護系統虛擬主機完成 Windows update 作業，未完成者，每次記 1 點，超過 3 點(不含 3 點)以上每增加 1 點懲罰性罰款 3 仟元整。

（九）廠商駐點人員使用之電腦，未於下班時間關機，無正當理由，經清查列表者，每次罰款 1 仟元整。

柒、 相關表單：(依機關資安規定表單為原則並以電子檔方式提供)

一、資訊系統維護服務單

二、應用系統變更申請紀錄表

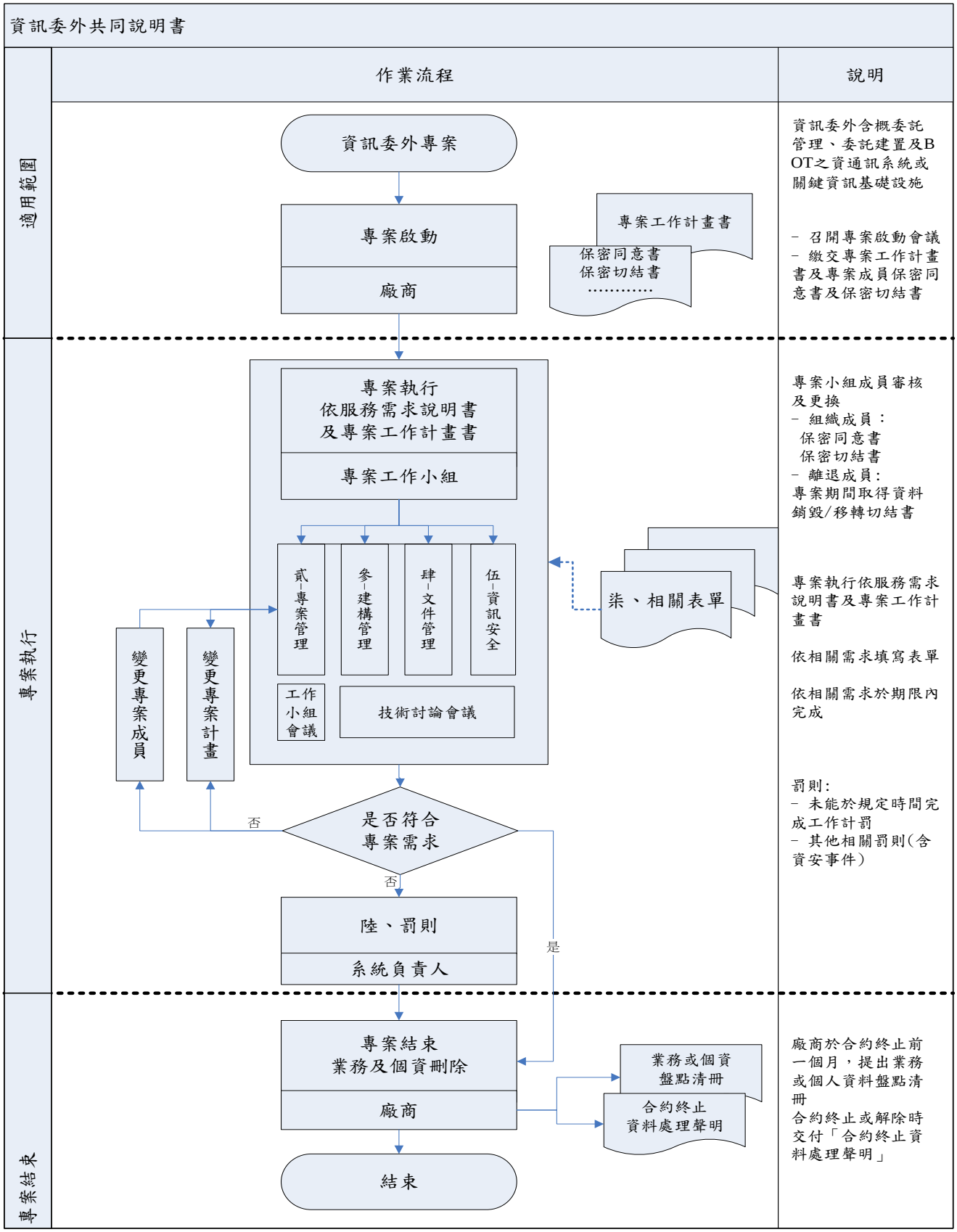
三、資訊安全異常處理單

四、委外廠商稽核評估表

五、未依規定時間完成工作計罰天數之計算說明表

六、資訊資產清冊
七、災難復原演練計畫
八、災難復原演練紀錄
九、會議紀錄
十、會議前準備文件檢查清單
十一、Table 增加 9 個欄位
十二、「程式設計之細部設計說明」文件撰寫範例
十三、駐點人員請假單
十四、電腦使用申請表
十五、軟體使用切結書
十六、保密同意書
十七、保密切結書
十八、資訊業務委外廠商資訊安全聲明書
十九、同意不將專案移至境外執行聲明書
二十、程式碼安全弱點掃描申請單
二十一、弱點掃描申請暨修補處理單
二十二、系統開發流程
二十三、遠端連線服務申請表及動態密碼異動紀錄
二十四、遠端連線存取使用紀錄表
二十五、GCB 例外原則申請單
二十六、專案期間取得資料銷毀/移轉切結書
二十七、合約終止資料處理聲明
二十八、防護基準選用暨執行措施表(普)
二十九、防護基準選用暨執行措施表(中)
三十、防護基準選用暨執行措施表(高)
三十一、風險辨識、分析與對策表
三十二、業務利害關係調查表
三十三、資訊系統安全等級評估表

捌、 作業流程圖：


資訊委外共同說明書
適用範圍
作業流程
說明
資訊委外專案
專案啟動
廠商
專案工作計畫書
保密同意書
保密切結書
……
資訊委外含概委託管理、委託建置及BOT之資通訊系統或關鍵資訊基礎設施
- 召開專案啟動會議
- 繳交專案工作計畫書及專案成員保密同意書及保密切結書
專案執行
專案執行
依服務需求說明書
及專案工作計畫書
專案工作小組
貳-專案管理
參-建構管理
肆-文件管理
伍-資訊安全
工作小組會議
技術討論會議
變更專案成員
變更專案計畫
柒、相關表單
專案小組成員審核及更換
- 組織成員：
保密同意書
保密切結書
- 離退成員:
專案期間取得資料銷毀/移轉切結書
專案執行依服務需求說明書及專案工作計畫書
依相關需求填寫表單
依相關需求於期限內完成
否
是否符合
專案需求
否
是
罰則:
- 未能於規定時間完成工作計罰
- 其他相關罰則(含資安事件)
陸、罰則
系統負責人
專案結束
專案結束
業務及個資刪除
廠商
業務或個資盤點清冊
合約終止
資料處理聲明
結束
廠商於合約終止前一個月，提出業務或個人資料盤點清冊
合約終止或解除時交付「合約終止資料處理聲明」