# 衛生福利部國民健康署資通安全條款

中華民國 94 年 1 月 24 日核定
中華民國 94 年 3 月 07 日修訂
中華民國 96 年 2 月 15 日修訂
中華民國 97 年 10 月 21 日修訂
中華民國 98 年 2 月 12 日修訂
中華民國 98 年 9 月 21 日修訂
中華民國 101 年 10 月 15 日修訂
中華民國 102 年 9 月 23 日修訂
中華民國 104 年 2 月 12 日修訂
中華民國 104 年 9 月 30 日修訂
中華民國 105 年 1 月 11 日修訂
中華民國 105 年 10 月 15 日修訂
中華民國 106 年 8 月 28 日修訂
中華民國 109 年 4 月 1 日修訂
中華民國 110 年 8 月 16 日修訂
中華民國 111 年 6 月 9 日修訂
中華民國 112 年 10 月 18 日修訂

一、廠商（委外計畫主持人及其所屬員工、協力廠商，以下簡稱乙方）承諾於原契約有效期間內及期滿或終止後，對於所得知或持有本署（以下簡稱甲方）之公務機密與資通系統(網站)相關資料，應刪除或銷毀執行服務所持有本署之相關資料，或依本署之指示返還或移交之，並保留執行紀錄。專案履約期間非經甲方事前書面同意，乙方不得為本人或任何第三人複製、保有、利用該等公務秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等公務機密，或對外發表或出售。

二、乙方因承辦業務所獲得之資訊，應依個人資料保護法及相關法令規章恪遵保密規定，並應簽署「附件 1-保密切結書」(如已簽署本署資訊服務採購契約中之保密相關文件，則以契約為主)，如有違失，由乙方負全部責任，責任說明如下：

（一）刑事責任方面，依據刑法及個人資料保護法等相關規定，受甲方委託之乙方人員雖不具公務員身分，但依據個人資料保護法第 4 條之規定，受本署委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同本署。

（二）民事責任方面，違失事由，歸屬乙方，乙方應負完全損害賠償責任。

（三）行政責任方面，政府採購法第 101 條第 1 項第 12 款規定，因可歸責於乙方之事由，致解除或終止契約者，招標單位應將乙方刊登於政府採購公報上，同法第 103 條第 1 項第 2 款規定，經刊登在政府採購公報上之乙方，於通知日起前五年內未被任一機關刊登者，自刊登之次日

起三個月；已被任一機關刊登一次者，自刊登之次日起六個月；已被任一機關刊登累計兩次以上者，自刊登之次日起一年，無法參加所有政府採購之招標。但經判決撤銷原處分者，應註銷之。

三、乙方應與參與人員訂定工作契約，乙方及其協力廠商有義務告知，並要求參與人員嚴守工作契約內容及甲方業務機密；乙方及其參與人員應切實依據原契約內容執行業務，執行業務過程中若造成第三人權益損失，概由乙方負責。

四、乙方需將參與人員名單與工作項目及權限造冊列管並交付甲方備查，專案團隊成員不得為陸籍人士。人員、項目及權限如有異動時，需於 3 日內主動將異動資料以書面函報機關，人員異動流程依「附件 2-委外專案成員異動流程圖」辦理。

五、乙方依原契約提供甲方服務時，所產生、取得或持有甲方之資料，包括文字、影像、圖形、聲音，不論其儲存於印刷、磁性、光學或其他媒體上，皆屬於甲方所有。除非為提供服務所需，或經甲方書面同意，不得複製、揭露或交付第三人。

六、乙方承辦甲方業務如涉及資通系統(網站或資料庫)開發、維護、維運及其他相關作業，或可接觸甲方資訊環境時，不得於甲方之任何資訊系統或新開發之資訊系統植入木馬程式，或開啟程式後門漏洞，亦不得未經甲方授權任意刪除或更改原有帳號權限及自行開立新帳號存取系統資源及執行弱點掃描等作業。

七、乙方若將契約主要工作項目(包含資通服務或資通系統開發、維運及改版相關工作項目)分(轉)包第三方廠商，請提報本署分包之工作項目及繳交第三方廠商保密切結書，其分包契約內需包含本署資通安全要求事項。

八、乙方承辦甲方業務如涉及資通系統(網站或資料庫)開發、維護、營運及其他資訊相關作業應依下列項目擬具具體作法，經甲方確認同意後辦理：

（一）資訊安全組織

1. 依人員權責及職務分別訂定其安全責任。
2. 與相關單位如主管機關、資訊服務廠商、檢警單位、電力單位、電信單位及消防救災單位建立聯絡管道。
3. 乙方之協力廠商契約應包含法律需求（如個人資料保護法與資通安全管理法）、界定雙方有關人員權責、使用安全控管措施及作業程序、對委外廠商資安稽核權等條文。

（二）人力資源安全

1. 對於可存取機密性、敏感性資訊或系統之人員以及配賦系統存取特別

權限之人員妥適分工，分散權責。

2. 人員（含第三方使用者）之調動、離職或退休，除第四條規定外，應取消、停用或調整其識別碼、通行碼、存取權限及安全責任，並繳回其使用或保管之資訊資產(若需保留帳號供後續交接人員使用，需另外向資訊業務主管單位提出申請)。
3. 人員應接受適當的資通安全暨個資保護訓練。

（三）資產管理

1. 需整理與本專案相關之資訊資產清冊，如有異動應更新後副知甲方承辦人員。
2. 各項資訊資產需有明確的管理者及使用者。
3. 乙方於專案範圍內不得提供及使用大陸廠牌資通訊產品。

（四）實體與環境安全

1. 界定專案範圍內重要實體區域並施予安全保護。
2. 重要實體區域的進出權限應定期審查並更新。
3. 人員進入重要實體區域實施安全控制措施及監督其活動並保留進出紀錄。
4. 重要實體區域應設置安全設備（如消防設施）且定期檢查並做成書面紀錄留存查考。
5. 重要實體區域與易燃物或危險物品保持安全距離。
6. 專案如涉及電腦機房管理，需隨時掌握機房溫度及溼度狀況。
7. 電腦機房操作人員需熟悉滅火系統操作方法及滅火器位置。
8. 設備送場外維修，須經甲方承辦人員及權責主管同意，對於儲存之資訊需有適當安全保護措施。
9. 設備報廢前須經甲方承辦人員及權責主管同意，將專案之機密性、敏感性資料及授權軟體予以移除。
10. 資訊資產如須攜出場外使用，需均經事前授權，並作安全查核。
11. 機密性、敏感性資訊儲存媒體在不使用或不在班時需妥為存放。
12. 為確保設備不遭受損壞、線路被破壞或拔除及電源或其它設施因失效而中斷，應對設備、線路及支援設施(如空調水電等)定期維護檢查。
13. 另設備已向上集中至衛福部機房者，實體與環境安全規定則依循衛福部機房管理規定辦理。

（五）存取控制

1. 本署資通系統(網站)密碼設定最少要有 12 個字元，並符合複雜性原則，內含英文字母大寫或小寫、阿拉伯數字及特殊字元（如!@#$）至

少 3 種，且不可與帳號完全相同或相似，及避免使用個人資料作為密碼；避免使用有意義的字串；每 90 天須更改一次密碼；更換密碼時，不得與前 24 次之密碼重複且至少有三個字元不同；密碼輸入錯誤次數超過 5 次即鎖定用戶登錄作業 15 分鐘；應遮蔽鑑別過程中之資訊，例如以特殊符號代替使用者鍵入之密碼;另資通系統(網站)作業系統主機之密碼原則設定，則依主管機關最新公告之組態基準(Government Configuration Baseline，簡稱 GCB)為準。

2. 各作業系統（含公用程式）、資訊系統與資料庫及網路設備之使用需經過授權，且應有身分鑑別機制。資訊存取權限之設定以工作所需最小權限與最少資訊為原則。
3. 未經甲方同意不得新增或刪除系統帳號及異動權限，使用者職務異動時應重新檢核權限並提出權限異動申請，以符合最小權限要求。
4. 本署資通系統(網站)應執行帳號權限清查,配合本署資訊業務權責單位進行每半年應清查一次，並紀錄於「ISMS-204-01-01 帳號定期清查紀錄單」交付甲方承辦人員歸檔保存。
5. 本署資通系統(網站)帳號不得共用同一帳號或將帳號交付他人使用;如有例外情形(如:與應用系統連結相關者)需經權責主管同意後依系統特性或系統安全考量辦理，外借帳號使用後應立即變更密碼。
6. 帳號註冊及註銷程序需做成書面紀錄留存查考。
7. 因系統管理或特殊作業需要而設定特殊權限時，應做成書面紀錄留存查考。
8. 本署資通系統（網站）最高管理者權限一定要甲方持有，得授權同等權限予乙方進行建置、維護，使用者帳號權限如須異動應告知甲方並經核可後得進行異動。

（六）通訊與作業安全管理

1. 作業系統主機需使用防毒軟體或採用其他防護設備，並即時更新病毒碼，且定期對電腦系統及資料儲存媒體進行病毒掃描。
2. 重要電腦資料媒體（含報表）之運送，需有安全保護措施並留有完整監控紀錄（含收送人、時間及內容）。
3. 所有主機之作業系統時鐘需定期核對校正，以確保時間紀錄正確。
4. 軟體安裝完畢後應立即更新乙方或第三方供應商所預設之密碼及相關服務之設定。
5. 本署資通系統(網站)資料應依其等級遵循以下備份規定：
   5.1 資通系統安全等級「普」，資料備份頻率則不得低於每月 1 次完整備份及須保留至少三代以上備份資料。

5.2 資通系統安全等級「中」，資料備份頻率則不得低於每兩週 1 次完整備份及須保留至少三代以上備份資料。

5.3 資通系統安全等級「高」，資料備份頻率則不得低於每週 1 次完整備份及須保留至少三代以上備份資料。

備份資料需異地儲存，並定期進行回復測試，以確保備份資料之有效性。

6. 資料交換（無論是電子或實體交換）需經甲方核准，若涉及資料外釋則依本署「資料提供及使用作業要點」辦理(包含資料係屬機密敏感性質亦同)。

7. 應定期執行主機群弱點掃描作業，弱點掃描後應產生弱點掃描報告，屬於中、高風險之弱點應限期 14 日內回覆改善情形(含甲方執行之弱掃報告)，並填寫「ISMS-206-01-02 弱點處理報告單」，且於修補後進行複檢作業，另甲方定期執行弱點掃瞄之處理結果報告需列入驗收，若乙方違反上述條款，將納入記點辦理。

8. 不開放申請外部遠距作業，本署資通系統（網站）之各項維運作業應至機房作業，並提前向甲方申請。

9. 本署資通系統（網站）作業系統主機需留存詳細的管理者與操作員之作業日誌，至少包含主機安全稽核日誌及登出、登入日誌（正常登入、異常登入、登入失敗）等，並保存 6 個月以上；應用系統及網站之作業日誌，至少包含系統登入、登出日誌（正常登入、異常登入、登入失敗）、資料異動、資料查詢及應用程式日誌等，且針對管理者權限應留存各項功能操作紀錄日誌，並保存 6 個月以上。

10. 如設有防火牆等資安防禦設備，相關設定組態檔（config）應至少保留兩代，防火牆紀錄檔（log）應至少保留 6 個月，並視設備的支援程度，考量適當的匯出與保存的方式，應定期(每年至少一次)審查防火牆規則。

11. 應配合本署交辦之各項資通安全相關作業。

（七）系統獲取、開發及維護

1. 乙方應依據資通安全管理法之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，實作資通系統該等級之控制措施(配合填寫本署提供自評相關文件，確保實際情形符合法規)。

2. 乙方應於資通系統(網站)開發及變更時，遵循 SSDLC 安全軟體開發生命週期(參考資通安全責任等級分級辦法附表十資通系統防護基準之「系統與服務獲得」構面對應防護需求等級之各項控制措施)及下列各階段應留存之紀錄：

2.1 需求階段：甲乙方共同討論之需求訪談相關紀錄，並由雙方單位主管確認，如：會議簡報與紀錄或需求訪談確認單及 ISMS-207-01-05 系統需求資通安全檢核表。

2.2 設計階段：乙方針對需求階段之結論，評估與規劃系統使用量及擴充之可行性，需注意硬體設備及軟體系統版本更新、使用與維護之生命週期，及硬軟體系統運作相容性，提供甲方確認之需求模型或草案逕行確認，如：會議簡報與紀錄或開發功能規格書。

2.3 開發階段：乙方依據開發功能規格進行程式開發，過程中需注意安全需求實作必要控制措施，應注意避免軟體常見漏洞。

2.4 測試階段：

- 乙方需建置測試環境(原則上建置於署內環境)供雙方進行功能測試，測試區及正式區應進行區隔，測試作業需避免以真實資料進行(若需以真實資料測試，建議優先進行去識別化後進行測試，如無法進行去識別化，則應於測試完成後完全清除資料)測試完成後應留存測試紀錄，如：測試確認單或測試報告書（須雙方單位主管確認）。
- 經雙方確認測試功能無誤，乙方應執行技術性檢測確保其程式安全無虞，檢測之弱點應將中風險以上之弱點修補完畢，並留存紀錄，如：技術性檢測報告及修補紀錄文件。

2.5 部署階段：

- 協同議定新功能或變更功能之部署時間，並於資通系統(網站)提前進行停機公告事宜。
- 申請部署作業相關文件，並進行部署作業，如：系統(網站)變更紀錄暨上版單或 ISMS-208-01-01 資通系統問題需求處理單暨資安事件通報單。
- 確認部署完成後系統正常運作，進行版本變更管理作業，且更新資通系統(網站)相關文件。

3. 系統應定期執行維護(每月或每季)，維護內容應包含主機安全性更新(例：windows Update)、主機運作情形(主機硬碟剩餘容量檢視、CPU效能與記憶體監控紀錄、留存系統相關日誌、系統主機校時等)、防毒軟體掃描等作業、弱點掃描作業、檢視備份資料是否有效等，並將維護內容製作工報告交付本署備查。(如與本條款其他項目重複者，其作業方式依其所列描述為準)
4. 應對應用系統的資料登錄進行驗證，保證輸入資料的正確性及合理性。且須定期審查應用系統關鍵資料欄位或資料檔案的內容，確認其有效性和完整性。
5. 應使用合法授權技術與軟體，以避免侵害智慧財產權。.

6. 應定期確認系統軟體版本，對作業系統及應用系統進行任何版本升級或修補程式時，須對其進行審查和測試，以確保應用系統的穩定性與安全性；如因系統限制無法升級或修補，應提出因應措施。
7. 網站（系統）程式源碼與資料著作權及使用權之歸屬甲方一定要有使用權，著作權則由雙方協商決定（原則上為本署擁有）。
8. 如契約內需開發或維運本署資通網站(系統)案件，乙方需提供系統規格書(含系統硬體及功能架構、程式源碼說明、資料庫設計說明、使用第三方元件說明-需特別標註是否為 open source）、使用者操作手冊（含系統安裝、後端管理操作）、建置所需軟體、原始碼與執行碼列為必要驗收產品項目。
9. 乙方須確保契約內所開發及維護的本署資通系統(網站)憑證之有效性，並於到期前提早向承辦人報告，並辦理憑證更換事宜。
10. 乙方應針對契約內所開發及維護的本署資通系統(網站)完成主管機關最新公告之政府組態基準(GCB)導入作業，並持續維運。

（八）營運持續管理

1. 本署資通系統(網站)應建立營運持續計畫，填具「ISMS-209-01-01 營運持續計畫」及「ISMS-209-01-03 營運衝擊分析」，依不同情境進行復原規劃，以因應事故導致資訊服務系統中斷時，相關業務服務能持續提供。
2. 業務持續計畫應每年至少執行 1 次演練，並於演練結束後進行檢討，並產出「ISMS-209-01-02 復原演習紀錄」及「演練檢核表」，以確保計畫之有效性。

（九）上述作業應依資通安全管理法及其子法要求為優先作業與設定基準，如前述法規未規範，則依本署資通安全相關規定辦理。

九、乙方承辦甲方業務如涉及個人資料之蒐集、處理、利用或傳輸應依「個人資料保護法」及「附件 3- 衛生福利部國民健康署委外契約個資保護條款」辦理。

十、乙方進入甲方資訊資產存放場所作業或維修，如發生意外事件時，乙方應立即採取防範措施並立即通報甲方。意外發生如歸責於乙方，乙方應立即搶救、復原及採取重建措施，並對損害負起賠償責任。

十一、乙方如發生資通安全事件時，應第一時間通報甲方承辦人員，並填具「ISMS-208-01-01 資通系統問題需求處理單暨資安事件通報單」。

十二、乙方作業之檢查與稽核

（一）甲方視需要不定期派員實施查核乙方提供之服務是否符合本契約之規

定，乙方並應確實配合辦理，提供甲方書面資料及邀集相關人員列席備詢。上述查核得以不預告之方式進行之，乙方不得無故拒絕，有關稽核缺失乙方應限期改善不得推諉，如無正當理由未依限改善，以違約論。

（二）甲方必要時得委由專業之第三方或由主管機關、上級機關指示等，稽核乙方提供之服務，如：本署辦理之委外業務稽核、主管機關二者查核或上級機關之所屬機關稽核等。

（三）乙方得自行辦理一次以本案為範圍之資安稽核作業。（宜參考本署ISMS-315-01-02 委外業務個人資料保護例行檢查表(廠商使用)）

十三、智慧財產權

（一）乙方所有交付甲方之資訊系統及其有關文件、著作權及智慧財產權均屬甲方所有，甲方享有複製、散播、新增、修改、刪除等一切權利。

（二）乙方所有交付甲方研究成果報告，甲方享有複製、散播等權利，其著作權及智慧財產權，則依合約內容及相關法令辦理。

（三）乙方交付之本專案相關軟體項目中如包含第三者開發之產品，應切結保證（或提供授權證明文件）軟體使用之合法性（以符合中華民國著作權法規範為準），並提供手冊、磁片或光碟片（若為共享軟體，shareware，不在此限，惟仍應取得使用授權）。乙方如有隱瞞事實或使用未授權軟體之行為，致使甲方遭致任何損失或聲譽之損害時，乙方應負一切民事、刑事責任。

（四）乙方自行開發之電腦程式應提供系統軟體原始程式碼（若應用程式係由程式開發工具所開發，應將處理程序、鍵值定義及操作步驟等明列說明以替代原始程式碼）光碟片二份，經測試無誤後交由甲方保管，做為系統維護之用，系統相關軟體如有修改時應配合一併更新。系統開發過程甲方得指派人員參與，乙方應提供必要之指導及訓練，以協助軟體轉移順利進行。

十四、罰則

（一）乙方發生資通安全事件，經甲方認定事件嚴重程度達需通報行政院國家資通安全會報者，即依契約總價金千分之三計罰違約金；經甲方通知限期改善，屆期未改善者，按日處以契約總價金千分之一之違約金，得連續處罰至改善為止；但每一事件處罰違約金總金額不得超過契約總價金千分之十五。

（二）前款所述乙方發生之資通安全事件中，如涉及民眾隱私資料者，除依本條款第二點，由乙方擔負相關刑事、民事及行政責任之外，則依契

約總價金千分之五計罰違約金；經甲方通知限期改善，屆期未改善者，按日處以契約總價金千分之二之違約金，得連續處罰至改善為止；但每一事件處罰違約金總金額不得超過契約總價金千分之二十五。

（三）前述二款情形，如造成甲方任何損失，一切損害賠償與法律責任均由乙方承擔；若事件發生原因經甲方認定屬非可歸責於乙方者，得予免罰。

十五、本條款未盡事宜，依政府資訊公開法、個人資料保護法、個人資料保護法施行細則、資通安全管理法、資通安全管理法子法，以及其他相關法令辦理。

十六、檢附本署資通安全條款相關附件及紀錄表單:

附件 1-「保密切結書」。

附件 2-「委外專案成員異動流程圖」。

附件 3-「衛生福利部國民健康署委外契約個資保護條款」。

(其餘表單請逕向承辦人領取)

附件 1

# 資訊安全保密切結書（個人）

立切結書人　　（以下簡稱乙方）參與　　（以下簡稱甲方）辦理「○○委外案（以下簡稱專案）」，工作期間因業務需要接觸之公務（機密）資料，乙方願意依下列規定辦理：

一、乙方於專案進行期間因進行調查、搜集依合約所產生或所接觸之公務（機密）資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述公務（機密）資料，乙方須負保密責任。

二、公務（機密）資料保密期限，不受專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知公務（機密）資料，未經甲方同意或授權，不得洩漏或轉讓於第三者。

三、乙方雖不具公務員身分，但根據貪污治罪條例及個人資料保護法第 4 條之規定，乙方行為該當法條之構成要件，仍視為公務人員而加重處罰。

四、乙方及其協力廠商違反本資訊安全保密切結書之規定，致造成甲方或第三者之損害，乙方及其協力廠商應負民事、刑事責任，包括因此所致甲方涉訟所須支付之訴訟費用或對第三人賠償之金額。於第三人對甲方提出請求、訴訟，經接獲甲方書面通知，乙方及其協力廠商應提供相關資料。

此致

_____甲方

立切結書人

姓　　名：

身分證字號：

戶 籍 地 址：

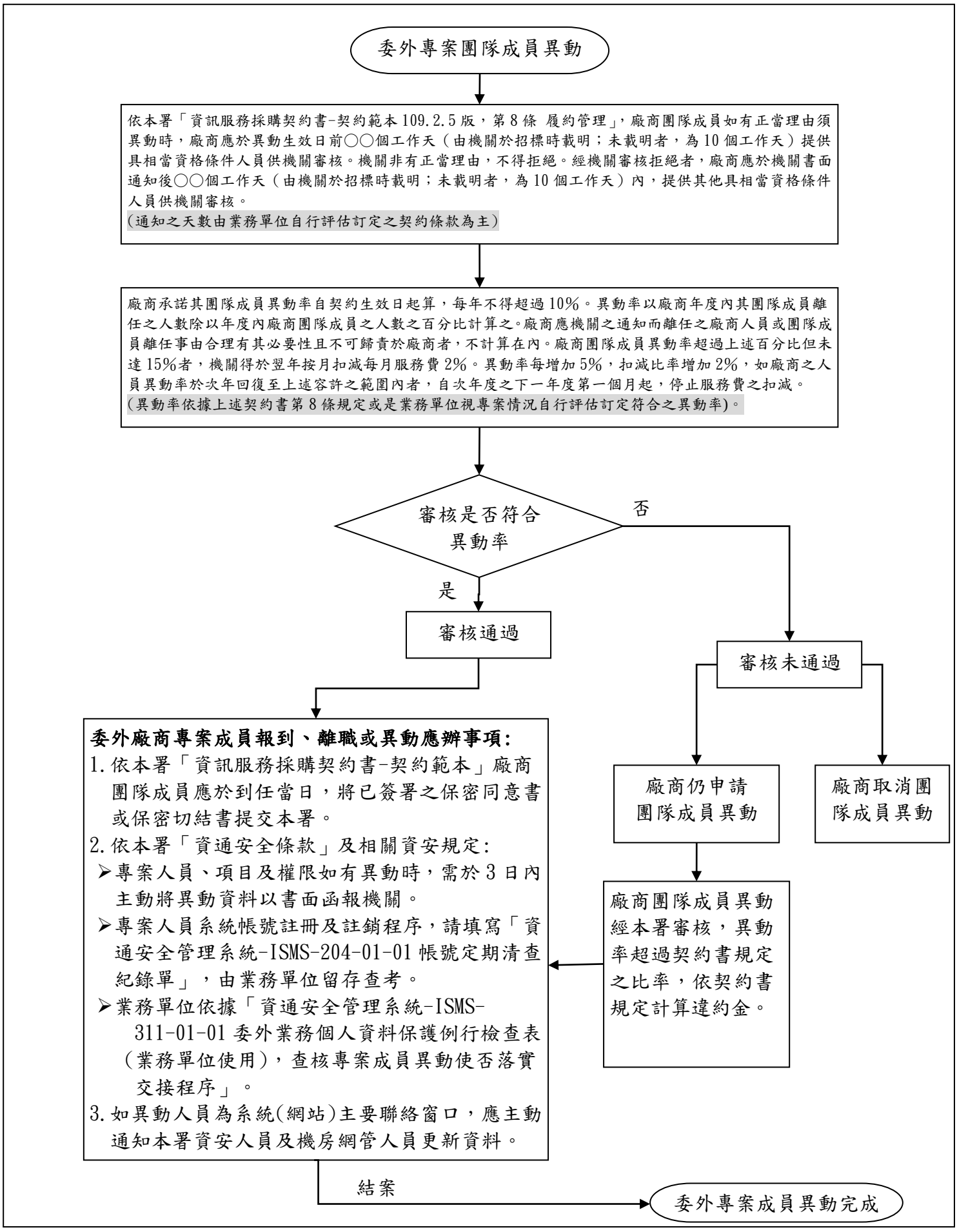
中 華 民 國　　年　　月　　日

個人資料蒐集告知:

以上之資料蒐集僅為作為資料保密切結之證明相關用途之必要範圍內，所進行蒐集、處理與利用當事人個人資料(屬於辨識個人者，包含姓名、身分證字號與聯絡方式)，本署將遵守法律規定保障當事人個人資料安全。另立切結書人享有個人資料保護法規定之相關權力。

附件 2

# 委外專案成員異動流程圖



附件 3

# 衛生福利部國民健康署委外契約個資保護條款

一、廠商僅得為辦理本契約所載委外業務之相關目的，蒐集、處理、利用或傳輸個人資料，並符合個人資料保護法、本署所訂定個資保護相關規範及其他相關法規命令。

二、廠商於本署所進行之個資保護相關作業活動，應依本署執行個資衝擊與風險分析結果所對應之個資管理流程與個資保護控制措施辦理之。廠商若有違反，致本署個人資料遭不法蒐集、處理、利用或其他侵害者，廠商應負損害賠償責任。

三、廠商員工於專案執行期間因進行調查、蒐集依合約所產生或所接觸之個人資料，非經本署同意或授權，不得以任何形式洩漏，或進行非法之蒐集、處理、利用或交付第三者。對所獲得或知悉之個人資料，廠商須負保護及保密之責任。

四、個人資料保密期限，不受專案工作完成（結案）及廠商不同工作地點及時間之限制，廠商所持有或所獲知之個人資料，未經本署書面同意或授權，不得洩漏或轉讓於第三者。

五、廠商於專案結束時，應依本署之要求進行個人資料之完整銷毀，非經本署書面通知許可，廠商不得私自保留、處理或利用執行專案所獲取之個人資料。

六、廠商違反本契約之規定，致個人資料外洩，造成機關或第三者之損害或賠償，廠商同意無條件負擔全部責任，包括因此所致本署或第三人涉訟，所須支付之一切費用及賠償。於第三人對機關提出請求、訴訟，經接獲本署書面通知，廠商應提供相關資料。

七、本署得保留對廠商實施個人資料管理稽核之權利，以確認廠商是否遵循個人資料保護法及落實本署相關個資管理規範。