**委外廠商資訊安全自我檢核表**

日期：　　年　　月　　日

公司名稱：

聯絡人姓名： 連絡電話： Email：

計畫名稱：

資通系統名稱：

防護需求等級：□普 □中 □高

資通系統/網站設備裝置地點：□本中心機房 □外部-放置地點：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

資料敏感程度：□一般業務資料 □敏感業務資料 □敏感個人資料 (可複選)

備註說明：本檢核表適用所有「普」等級及以上資通系統。

| **管理領域** | **項次編號** | **強化措施** | **自我檢核** | **現況說明**(符合/不符合/不適用均需說明) | **備註說明** |
| --- | --- | --- | --- | --- | --- |
| 實體環境安全管理 | 1 | 執行本案之系統使用雲端服務，應具備適當地雲端安全防護措施。 | 符　合不符合不適用 |  | 機房是否在國內，以及是否有做加密或帳號安全有強化(多因素認證)，機敏資料是否放置雲端。 |
| 2 | 資通系統部署於本中心以外之機房至少應符合以下要求：(一)機房運作通過ISO 27001驗證。(二)出入口及通道應設置監視器(錄影至少保存一個月以上)。(三)主機設備應安裝防毒軟體及架設網路防火牆。(四)機房維運人員每年應接受資安教育訓練。 | 符　合不符合不適用 |  |  |
| 網路安全管理 | 1 | 限制連線資通系統僅限於特定服務埠(port)。 | 符　合不符合不適用 | 現況說明範例：符合：使用80及443 port符合：本系統僅供內部使用，系統使用XX port |  |
| 2 | 主機管理人員如需於非資通系統所在的網路環境進行遠端維護管理，須經由加密網路連線操作，並使用雙因子驗證機制。 | 符　合不符合不適用 | 現況說明範例：符合：遠端連線須先建立VPN加密通道，整合動態密碼機制不適用：無遠端連線需求 |  |
| 3 | 應設置防火牆並網路架構應做適當網路區隔。 | 符　合不符合不適用 | 現況說明範例：符合：系統存放於客戶指定之機房，該單位設置防火牆並網路架構應做適當網路區隔。不符合：請具體說明 | 建議確認存放位置之網路防護機制 |
| 作業系統及主機管理 | 1 | 各伺服器應安裝防毒軟體，並設定自動更新病毒特徵碼。 | 符　合不符合不適用 | 現況說明範例：符合：系統存放於客戶指定之環境，該單位各伺服器已安裝防毒軟體，並設定自動更新病毒特徵碼。不符合：請具體說明 | 建議確認系統之防護機制 |
| 2 | 資料庫系統與資通系統須設置於不同實體或虛擬主機。 | 符　合不符合不適用 | 現況說明範例：符合：有放置在不同的虛擬主機不符合：目前資料庫系統與主系統是放置在同一個虛擬系統不適用：配合XXX單位規定 |  |
| 3 | 具機敏性資通系統之資料庫應留存至少六個月之稽核軌跡或日誌。 | 符　合不符合不適用 | 現況說明範例：符合：操作日誌保留xx以上不符合：請具體說明不適用：無機敏性系統不適用：配合XXX單位規定 | 建議確認系統需求規格 |
| 4 | 資通系統前台與後台須區隔，後台系統須限制於特定網段才能登入。 | 符　合不符合不適用 | 現況說明範例：符合：有設定IP白名單不符合：請具體說明不適用：系統無前後台不適用：配合XXX單位規定 | 建議確認系統需求規格 |
| 5 | 主機管理人員不得共用帳號密碼，作業系統及資料庫每年應至少執行一次管理者帳號清查。 | 符　合不符合不適用 | 現況說明範例：符合：請說明管理原則不適用：配合XXX單位規定 |  |
| 6 | 資料庫平臺應開啟主機防火牆，僅允許資通系統主機IP存取；資料庫管理人員應由限定IP存取。 | 符　合不符合不適用 | 現況說明範例：符合：有設定IP白名單不符合：請具體說明不適用：無資料庫系統不適用：配合XX單位規定 |  |
| 7 | 作業系統更新應每月進行評估其需要性，經測試後再執行更新。 | 符　合不符合不適用 | 現況說明範例：符合：請說明管理原則不符合：請具體說明不適用：配合XXX單位規定 | 建議確認作業系統之更新機制 |
| 8 | 每年定期執行弱點掃描並執行評估與修補。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施不適用：委託單位無此要求 | 建議依據委託單位之需求確認此項要求 |
| 9 | 每半年進行伺服器安裝軟體清查，並確認軟體版本是否需更新。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施不適用：委託單位無此要求 | 建議依據委託單位之需求確認此項要求 |
| 資通系統管理 | 1 | 須符合防護需求等級之防護基準。 | 符　合不符合不適用 | 現況說明範例：不符合：請具體說明改善措施 | 建議依據委託單位之需求確認此項要求 |
| 2 | 使用HTTPS並僅用TLS1.2 以上協定關閉TLS1.0及TLS1.1。 | 符　合不符合不適用 |  |  |
| 3 | 應維護資料庫關係表、系統程式設計規格書、系統維護手冊及系統使用手冊之更新，並每年進行檢核以確保後續承接受託者得以持續維運。 | 符　合不符合不適用 |  |  |
| 4 | 資通系統如提供使用者上傳檔案功能，應考慮使用以下控制措施，以避免被有心人士惡意使用，成為入侵系統的管道：(一)限制可執行功能之使用者，或檢核來源IP限制具有風險的國家網段使用此功能。(二)設置檔案白名單，如：限制上傳檔案之副檔名，並針對檔案標頭及副檔名格式進行檢核。(三)使用者完成上傳後，系統立刻執行檔案更名。(四)系統自動將上傳檔案進行格式轉換，如：jpg檔案格式轉換為png檔案格式。(五)檔案上傳完成後，立即將檔案轉移到權限受限的目錄下。 | 符　合不符合不適用 |  |  |
| 5 | 落實程式(系統)版本更新管理程序，並留存相關紀錄。 | 符　合不符合不適用 |  |  |
| 6 | 每年辦理資通系統弱點掃描，中風險(含)以上弱點應修補。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施不適用：委託單位無要求弱點掃描 | 建議依據委託單位之需求確認此項要求 |
| 7 | 具機敏性資通系統應每二年辦理資通系統滲透測試，發現中風險(含)以上弱點應修補。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施不適用：委託單位無要求滲透測試 | 建議依據委託單位之需求確認此項要求 |
| 8 | 弱點掃描及滲透測試發現之弱點修補，未於規定期限內完成修補並執行複測通過者，應由機關列管追蹤。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施不適用：委託單位無要求弱點掃描及滲透測試 | 建議依據委託單位之需求確認此項要求 |
| 9 | 每年定期維護第三方元件清冊(包含元件項目、版本、授權及來源)。有弱點之第三方元件應更新為安全版本，六個月內未完成改善者，應提出未能更新版本之補償性控制方案，由機關列管。 | 符　合不符合不適用 |  |  |
| 災害復原演 | 1 | 每年至少執行一次災害復原演練，於演練後進行檢討並留下演練紀錄。 | 符　合不符合不適用 | 現況說明範例：符合：配合XXX單位規定(請說明執行頻率及內容)不符合：請具體說明改善措施(例：暫無預算，目前每天雲端本機備份，並定期備份還原演練)不適用：委託單位無要求災害復原演練 | 建議依據委託單位之需求確認此項要求 |
| 個人資料保護 | 1 | 任何形式儲存個人資料時應加密保護。 | 符　合不符合不適用 |  |  |
| 2 | 系統顯示個人資料時，應有遮蔽保護機制；如有特殊需要存取原始資料，須留下紀錄。 | 符　合不符合不適用 |  |  |
| 3 | 不使用真實資料進行測試，需以測試資料、替換或變更順序等去識別化方式進行使用。 | 符　合不符合不適用 |  |  |
| 委外廠商管理 | 1 | 同意定期對資通系統維護廠商及託管機房進行稽核。 | 符　合不符合不適用 |  |  |
| 2 | 原則上禁止廠商遠端連線至內部資通環境作業；如「業務需要需採遠端連線時，須經本中心同意且務必搭配雙因子認證機制，否則應立即停止使用。 | 符　合不符合不適用 |  |  |
| 3 | 保密切結(機密性)：針對參與系統開發或維護相關作業之員工、雇員、分包商及臨時等相關人員要求簽署保密切結書（同意書）。 | 符　合不符合不適用 |  |  |
| 4 | 委外關係終止或解除時，同意返還、移交、刪除或銷毀履行契約而持有之資料 | 符　合不符合不適用 |  |  |
| 5 | 使用本中心資訊案事務承攬合約書範本 | 符　合不符合不適用 |  |  |
|  | 6 | 本專案團隊人員是否具備資通安全專業證照，並檢附證照影本 | 本專案具備資通安全專業證照之團隊成員有：　位。(請檢附影本)本專案團隊成員未具備資通安全專業證照 |  |