

個人資料委外廠商檢查表

專案名稱：

廠商名稱：

填表說明：

一、查核結果欄：依查核實際狀況，參考相關佐證資料填具查核結果。

- (一) 符合：實際作業已依查核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。
- (二) 建議事項：經查核未發現不符合情形，但仍有可持續改善或優化之處，建議列入後續精進。
- (三) 部分不符合：對應稽核項目能夠提供相關紀錄，但紀錄有少數缺漏或人員執行時有疏失。
- (四) 不符合：未能提出執行稽核項目要求之作業程序、實作紀錄或相關文件紀錄缺漏甚多。
- (五) 不適用：實際作業排除查核內容之適用。

二、說明欄位：應記錄查核之參考佐證資料，或簡述實際作業狀況。

查核項目	查核內容	查核結果	說明
1. 人員及資源配置	1.1 配置專責人員或組織？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	1.2 配置適當資源？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
2. 界定個人資料	2.1 進行個資盤點？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	2.2 個資盤點是否確實？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	2.3 建立盤點清冊？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

查核項目	查核內容	查核結果	說明
3. 風險評估	3.1 進行風險評估？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	3.2 製成風險評鑑表？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	3.3 針對風險進行因應？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
4. 事件通報應變	4.1 有通報及應變程序？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	4.2 事件發生時確實通報？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	當年度無事故者， 4.2-4.6 應填不適用
	4.3 事件發生後採取應變措施？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	4.4 於期限內通知當事人？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	4.5 事後採取預防措施？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	4.6 將事件處理情形通知本會或相關單位？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
5. 蒐集處理利用之內部管理程序	5.1 資料蒐集、處理具備特定目的並具有法定要件？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.2 依規定取得當事人同意（當事人同意之情形）？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.3 履行告知義務（未履行告知義務時，是否符合免告知之情形）？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

查核項目	查核內容	查核結果	說明
	5.4 個人資料之利用，符合特定目的之範圍？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.5 是否有目的外之利用？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.6 目的外利用是否符合法定要件？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.7 是否利用因執行本契約所蒐集之個人資料進行行銷？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.8 是否提供個人資料予第三人？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.9 是否有進行複委託，進行前是否得機關同意並經複委託廠商簽訂保密協議？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	無複委託應填不適用
	5.10 對複委託方進行監督？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	無複委託應填不適用
	5.11 當事人權利行使流程？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.12 將當事人權利行使回覆情形做成紀錄供機關備查？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.13 契約終止或解除，是否刪除、銷毀所持有之個人資料？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.14 契約終止或解除，是否返還個人資料之載體？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
6. 資料安全與人員管理	6.1 是否進行去識別化作業？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

查核項目	查核內容	查核結果	說明
	6.2 是否有資料存取控制措施？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	6.3 是否進行加密？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	6.4 資料之傳送是否進行管控？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	6.5 保有資料者是否遵守保密協定？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	6.6 人員進出情形是否具體掌控？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
7. 認知宣導與教育訓練	7.1 是否確實進行認知宣導與教育訓練？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	7.2 是否進行課後評量？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	7.3 是否對新進人員進行教育訓練？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
8. 設備安全管理	8.1 是否對設備及環境進行控管與保護？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	8.2 是否定期檢查或維護更新設備？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
9. 稽核機制	9.1 是否設有稽核制度？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	9.2 是否定期實施稽核？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
10. 紀錄保存	10.1 是否保存個資管理紀	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項	

查核項目	查核內容	查核結果	說明
	錄？	<input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
11. 持續改善	11.1 是否定期檢視個資保護措施？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	11.2 是否針對缺失進行改善？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	11.3 是否依本會或稽核單位所提出之建議進行改善？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

資訊系統委外開發廠商增列查核項目

查核項目	查核內容	查核結果	說明
1. 安全系統設計原則	1.1 是否已制訂系統發展生命週期的安全設計原則，並實作於資訊系統？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	1.2 應用程式編碼時，是否已參考 OWASP 組織每年公告之撰寫程式的安全原則(Secure Coding Principles)或國家資通安全研究院之技術公告，以提升編碼之安全性？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	1.3 網頁應用程式編碼時，是否已參考 OWASP 組織每年公告之安全風險議題，避免撰寫不當產生風險？ 如：跨網站的指令碼(Cross Site Scripting)、注入缺失(Injection Flaw)、惡意檔案執行(Malicious File Execution)、不安全的物件參考(Insecure Direct Object Reference)及跨網站的偽造要求(Cross-Site Request Forgery)等不安全源碼之問題。	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

查核項目	查核內容	查核結果	說明
2.安全開發環境	2.1 系統開發環境是否有適當的保護？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	2.2 系統開發所使用的輔助工具軟體安全性是否進行評估？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	2.3 系統開發所使用之電腦是否定期執行各項漏洞修補程式或安全性更新？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	2.4 系統開發所使用之電腦是否全面使用防毒軟體並即時更新病毒碼？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
3.測試資料的保護	3.1 測試作業是否避免以真實資料進行？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	3.2 如須使用真實資料進行測試是否有進行實體隔離或存取權限管制？	<input type="checkbox"/> 符合 <input type="checkbox"/> 建議事項 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	