個人資料委外作業查核檢查表

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）不符合：完全未依查核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三）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 是否已配置專責人員或組織管理及維護保有之個人資料？	□符合□不符合□不適用	
	1.2 配置適當資源？	□符合□不符合□不適用	
2.界定個人資料	2.1 是否定義個人資料並建立盤點清冊？	□符合□不符合□不適用	
	2.2 個人資料是否包含特種個資？若有，是否詳述其法令依據及蒐集內容？	□符合□不符合□不適用	若未蒐集特種個資則填不適用
	2.3 個資盤點是否確實？	□符合□不符合□不適用	
3.風險評估	3.1 進行風險評估？	□符合□不符合□不適用	
	3.2 製成風險評鑑表？	□符合□不符合□不適用	
	3.3 針對風險進行因應？	□符合□不符合□不適用	
4.事故通報應變	4.1 有通報及應變程序？	□符合□不符合□不適用	
	4.2 事故發生時確實通報？	□符合□不符合	當年度無事故

查核項目	查核內容	查核結果	說明
		□不適用	者，4.2-4.6 應填不適用
	4.3 事故發生後採取應變措施？	□符合□不符合□不適用	
	4.4 於期限內通知當事人？	□符合□不符合□不適用	
	4.5 事後採取預防措施？	□符合□不符合□不適用	
	4.6 將事故處理情形通知機關？	□符合□不符合□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？	□符合□不符合□不適用	
	5.2 依規定取得當事人同意（當事人同意之情形）？	□符合□不符合□不適用	
	5.3 是否清楚直接或間接蒐集個人資料之適法性，如履行告知義務及時點（未履行告知義務時，是否符合免告知之情形）？	□符合□不符合□不適用	
	5.4 告知內容是否包含個資法第八條規定項目？	□符合□不符合□不適用	若符合個資法第八條第二項或第九條免告知則填不適用
	5.5 個人資料之利用，符合特定目的之範圍？	□符合□不符合□不適用	
	5.6 是否已訂定個人資料蒐集、處理及利用目的消失或屆滿之資料銷毀、刪除程序？	□符合□不符合□不適用	
	5.7 是否有定期檢核及記錄以確認特定目的外之利用？	□符合□不符合□不適用	
	5.8 目的外利用是否符合法定要	□符合□不符合	

查核項目	查核內容	查核結果	說明
	件？	□不適用	
	5.9 是否利用因執行本契約所蒐集之個人資料進行行銷？	□符合□不符合□不適用	
	5.10 是否提供個人資料予第三人？	□符合□不符合□不適用	
	5.11 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？	□符合□不符合□不適用	無複委託應填不適用
	5.12 是否定期對複委託方進行監督並記錄？	□符合□不符合□不適用	無複委託應填不適用
	5.13 當事人權利行使流程？	□符合□不符合□不適用	
	5.14 將當事人權利行使回覆情形做成紀錄供機關備查？	□符合□不符合□不適用	
	5.15 是否清楚瞭解個人資料之使用及其保存期限？	□符合□不符合□不適用	
	5.16 契約終止或解除，是否刪除、銷毀所持有之個人資料？	□符合□不符合□不適用	
	5.17 契約終止或解除，是否返還個人資料之載體？	□符合□不符合□不適用	
	5.18 員工離職時，是否依規定繳回其使用或保管之資訊資產（如個人電腦、隨身碟）？	□符合□不符合□不適用	
	5.19 新承接人員是否有變更各系統密碼？	□符合□不符合□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？	□符合□不符合□不適用	
	6.2 是否有資料存取控制措施？	□符合□不符合□不適用	
	6.3 是否進行加密？	□符合□不符合	

查核項目	查核內容	查核結果	說明
		□不適用	
	6.4 資料之傳送是否進行管控？	□符合□不符合 □不適用	
	6.5 使用資訊系統或其他系統進行個人資料交換時，是否有採取適當保護措施（如傳輸過程中進行加密）？	□符合□不符合 □不適用	
	6.6 是否有遠端存取控管措施（如限制遠端存取個人資料、傳輸過程加密）？	□符合□不符合 □不適用	如無開放遠端存取應填不適用
	6.7 保有資料者是否遵守保密協定？	□符合□不符合 □不適用	
	6.8 人員進出情形是否具體掌控？	□符合□不符合 □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？	□符合□不符合 □不適用	
	7.2 是否進行課後評量？	□符合□不符合 □不適用	
	7.3 是否對新進人員進行教育訓練？	□符合□不符合 □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？	□符合□不符合 □不適用	
	8.2 是否定期檢查或維護更新設備？	□符合□不符合 □不適用	
	8.3 是否針對存放個人資料之媒體於報廢或再利用前進行處理（如硬碟消磁）？	□符合□不符合 □不適用	
9.稽核機制	9.1 是否設有稽核制度？	□符合□不符合 □不適用	
	9.2 是否定期實施稽核？	□符合□不符合	

查核項目	查核內容	查核結果	說明
		□不適用	
10.紀錄保存	10.1 是否保存個資（含紙本及數位檔案）管理紀錄（如存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄）？	□符合□不符合 □不適用	
	10.2 受委託管理含有個人資料之資訊系統，是否已建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？	□符合□不符合 □不適用	
11.持續改善	11.1 是否定期檢視個資保護措施？	□符合□不符合 □不適用	
	11.2 是否針對缺失進行改善？	□符合□不符合 □不適用	
	11.3 是否依機關所提出之建議進行改善？	□符合□不符合 □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？	□符合□不符合 □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）或行政院國家資通安全會報技術服務中心之技術公告，以提升編碼之安全性？	□符合□不符合 □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？	□符合□不符合 □不適用	

查核項目	查核內容	查核結果	說明
	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。		
2.安全開發環境	2.1 系統開發環境是否有適當的保護？	□符合□不符合□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？	□符合□不符合□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？	□符合□不符合□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？	□符合□不符合□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？	□符合□不符合□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？	□符合□不符合□不適用	