委外廠商查核項目表 Outsourcing manufacturer inspection item list

ISPI-D-065，機密等級 Level of confidentiality：2限閱 · 版　　本 Version：1.0

紀錄編號. / NO　　填表日期. / Date.

案件名稱	**(如、合約、採購案或計畫名稱)**		
查核對象 **(公司或組織名稱)**	**(請加蓋公司印鑑)**		
負責人	**(加蓋負責人印鑑)**		
往來關係	□採購/維護案 □合作計畫	**查核類別**	□實地訪查 □遠距檢核
本校查核人員	**(請購時由請購單位承辦人員擔任)**	**查核日期**	

填表說明：

一、受委託者處理業應依循「個人資料保護法施行細則」第8條及「資通安全管理法施行細則」第4條辦理，進行個資及資通安全管理識別，受委託廠商應依法接受本校及相關上層指導單位，進行個資及資安措施監督查核作業，必要時委託者得進行實地訪查。

二、查核欄位-廠商自評、本校查核：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。

三、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。

四、查核項目表僅提供各權責單位對於委外作業廠商資訊安全暨個人資料保護管理符合度的有效性查檢。

五、每一查核項目均應填具，查核對象已具備相關驗證範圍之有效期內個人資料保護制度驗證證明 (如、ISO27001、ISO27701通過證書)，可進行抽樣式檢核。

編號 ***個資專屬** **#資安專屬**	**查核內容**	**廠商自評**			**本校查核**			**說明**
		符合	**不符合**	**不適用**	**符合**	**不符合**	**不適用**	
1	是否瞭解本校之資安暨個資保護管理政策及目標？	□	□	□	□	□	□	
2	是否訂定本專案相關工作之責任分工？	□	□	□	□	□	□	
3	專案執行人員是否具備相關專業資安證照或相關業務輔導經驗？	□	□	□	□	□	□	
4	是否依本校規定，完成保密切結書或其他契約化協議書之簽署？ (若為請購程序前的評核，則於說明欄註明，並選擇不適用)	□	□	□	□	□	□	

編號 *個資專屬 #資安專屬	查核內容	廠商自評			本校查核			說明
		符合	不符合	不適用	符合	不符合	不適用	
*5	是否與本校業務權責單位確認本案業務使用或接觸之個人資料保護之項目檔案，並建立有個人資料項目清冊。 (若業務權責單位評核本案查核對象不會直接或間接接觸個人資料，則於說明欄註明，選擇不適用)	□	□	□	□	□	□	
*6	承5，是否包含特種個資，並有其法令依據及蒐集內容？。(若無特種個資則選擇不適用)	□	□	□	□	□	□	
*7	承5，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）	□	□	□	□	□	□	
8	本案是否有進行複委託，進行前是否得本校業務權責單位同意並經複委託廠商簽訂保密協議？	□	□	□	□	□	□	
9	專案人員離職或轉調時，是否向本校提報，並歸還所有機敏資訊資產，並終止其存取權限？	□	□	□	□	□	□	
10	對於資通系統或資訊設備之使用帳號是否提出申請，並有進行定期審核？	□	□	□	□	□	□	
11	承上，帳號是否與其他單位不一樣，且密碼長度至少10碼以上，並符合密碼複雜度原則？	□	□	□	□	□	□	
#12	資通系統提升需求規劃、版本或韌體更新時，是否與本校權責單位溝通確認，並留存討論紀錄？	□	□	□	□	□	□	
#13	承上，其需求規劃是否將「資通安全責任等級分級辦法」附表十防護基準控制措施列入考量？	□	□	□	□	□	□	
#14	執行資通系統之變更作業時，是否有依規定留存變更紀錄或記錄於工作日誌中？	□	□	□	□	□	□	
#15	是否依規定進行版本控管，如程式原始碼等？	□	□	□	□	□	□	
#16	是否辦理安全性檢測作業(如網站安全弱點掃描、系統滲透測試)?	□	□	□	□	□	□	
#17	是否定期取得系統漏洞資訊，與本校權責單位溝通後並採取必要措施？	□	□	□	□	□	□	

委外廠商查核項目表 Outsourcing manufacturer inspection item list

ISPI-D-065，機密等級 Level of confidentiality：2限閱， 版　　本 Version：1.0

編號 *個資專屬 #資安專屬	查核內容	廠商自評			本校查核			說明
		符合	不符合	不適用	符合	不符合	不適用	
#18	是否針對本校委外業務項目進行風險評估，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理?如考量版本是否有漏洞、是否需要備援機制、備份的週期、擺放位置對網路的影響及防火牆設定政策等。	□	□	□	□	□	□	
19	是否依規定監視系統各項資源之使用，以確保系統效能之可用性？	□	□	□	□	□	□	
20	是否產生、保存與定期審查記錄系統活動、異常、錯誤及資訊安全事件之事件日誌？	□	□	□	□	□	□	
21	是否依規定進行資訊、軟體及系統影像之備份作業？	□	□	□	□	□	□	
22	承上，備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	□	□	□	
23	是否配合本校執行營運持續演練，並留存執行紀錄？	□	□	□	□	□	□	
24	設備是否定期維護，以確保其可用性及完整性？	□	□	□	□	□	□	
25	設備送場外維修，對於儲存資訊是否有安全保護措施？如設備親送或維修廠商針對維護過程有安全管控措施。	□	□	□	□	□	□	
26	對於本校專案的敏感性、機密性資訊之傳送及保存是否採取資料加密等保護措施？	□	□	□	□	□	□	
27	連線校內系統之個人電腦是否有安全性管控，如windows update、安裝防毒軟體等？	□	□	□	□	□	□	
28	是否依規定，交付契約要求之各項文件或其他要求事項，以符合契約規範之服務水準指標(SLA)？	□	□	□	□	□	□	

編號 *個資專屬 #資安專屬	查核內容	廠商自評			本校查核			說明
		符合	不符合	不適用	符合	不符合	不適用	
29	是否依契約規定，針對服務緊急狀況或一般狀況，在規定時間內回覆並處理，以符合契約規範之服務水準指標(SLA)？ (若為請購程序前的評核，則於說明欄註明，並選擇不適用)	□	□	□	□	□	□	
30	是否規劃於委託關係終止或解除時，返還、移交、刪除或銷毀履行契約而持有之機敏資料，並提供相關證明紀錄?	□	□	□	□	□	□	
31	是否知悉本校資通安全事件通報應變程序，並配合規定辦理？	□	□	□	□	□	□	
32	執行委外業務時，違反個資或資通安全相關法令或知悉資通安全事件時，是否立即通知本校並採行補救措施？	□	□	□	□	□	□	
33	是否留有資通安全事件處理之記錄文件，並包含改善措施？	□	□	□	□	□	□	
34	是否依規定，提供事件或異常之改善情形？	□	□	□	□	□	□	
35	是否配合本校資通暨個資安全維護計畫或資安個資稽核等與本專案有關之稽核作業？	□	□	□	□	□	□	
36	承上，若有缺失是否配合本校改正稽核之缺失？	□	□	□	□	□	□	
資通訊系統委外開發廠商增列查核項目 (當專案為委外開發系統時，需評核以下項目，非委外開發請選填不適用)								
37	是否使用安全系統發展生命週期(SSDLC) 的安全設計原則，並實作於資訊系統？	□	□	□	□	□	□	
38	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）或政府機關公佈之技術公告，以提升編碼之安全性？	□	□	□	□	□	□	

編號 *個資專屬 #資安專屬	查核內容	廠商自評			本校查核			說明
		符合	不符合	不適用	符合	不符合	不適用	
39	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。	□	□	□	□	□	□	
40	系統開發環境是否有適當的保護？	□	□	□	□	□	□	
41	開發及測試環境是否有進行區隔?	□	□	□	□	□	□	
42	系統開發所使用的輔助工具軟體安全性是否進行評估？	□	□	□	□	□	□	
43	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？	□	□	□	□	□	□	
44	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？	□	□	□	□	□	□	
45	測試作業是否避免以真實資料進行？	□	□	□	□	□	□	
46	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？	□	□	□	□	□	□	

案件承辦單位，已確認前述資料正確性。　　註：陳核層級請權責單位依需求調整

本案業務權責單位承辦人用印 (請購單位承辦人或本校查核人員)

權責主管用印