附件 14 委外廠商查核項目表

○○○（機關名單）委外廠商查核項目表

編號：○○

填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派副首長擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	■	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	■	□	□	機關內部訂有資安責任分工組織。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	■	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	■	□	□	機關依規定配置資安人員2人。
	3.3 是否具備相關專業資安證照或認證？	■	□	□	專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？	□	■	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	■	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	■	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	■	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	■	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	■	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	■	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	■	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	■	□	□	按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	■	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	■	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	■	□	對於核心系統主機並未設置特別保護機制。
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	■	□	□	定期檢查物理面之風險。
	5.9 電源之供應及備援電源是否作安全上考量？	■	□	□	有設置備用電源。
	5.10 通訊線路及電纜線是否作安全保護措施？	□	■	□	電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護，以確保其可用性及完整性？	■	□	□	設備按期維護。
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	■	□	□	訂有相關之保護措施。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	■	□	□	攜帶式設備訂有保護措施。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	■	□	□	設備報廢前均有進行資料清除程序。
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	■	□	人員下班後並未將機敏性公文妥善存放。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	■	□	□	系統開發測試與正式作業區隔。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	■	□	□	按時更新病毒碼。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	■	□	□	定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？	■	□	□	定期進行漏洞修補。
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	■	□	□	系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？	■	□	□	有定期做備份處理。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	■	□	□	備份資料均有測試。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	■	□	□	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	■	□	□	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	■	□	□	訂有使用者存取權限註冊及註銷之作業程序。
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	■	□	未定期檢視使用者存取權限。
	5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	■	□	□	通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	■	□	□	通行碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	■	□	□	依規定訂定適當之存取權限。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	■	□	□	對於特定網路有訂定相關之控制措施。
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	■	□	□	有針對行動式電腦訂定管理政策。
	5.32 重要系統是否使用憑證作為身份認證？	■	□	□	針對重要系統設有身份認證。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	■	□	□	系統更新後相關措施仍有效。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	■	□	□	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	■	□	□	有訂定通報應變程序。
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	■	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	■	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	■	□	□	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	■	□	□	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	■	□	□	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	■	□	□	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護計畫實施情形	8.1 是否設有稽核機制？	■	□	□	訂有稽核機制。
	8.2 是否定有年度稽核計畫？	■	□	□	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	■	□	□	有按期執行稽核。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
之精進改善機制	8.4 是否改正稽核之缺失？	■	□	□	訂有稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	■	□	□	有訂定持續改善措施。
	10.2 是否追蹤過去缺失之改善情形？	■	□	□	有追蹤缺失改善之情形。
	10.3 是否定期召開持續改善之管理審查會議？	■	□	□	定期召開管理審查會議。

單位主管：陳○○　　資通安全長[1]：林○○

註：陳核層級請機關依需求調整

[1] 特定非公務機關部分，可能是其資安代表，或單位之資安負責人員。