附件二：

教育部國教署所轄公務機關109年度資通安全維護計畫
實施情形查核表

單位：

查核日期：　年　月　日

查核人員：

查核項目	查核內容	查核結果			準備資料或客觀證據
		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？	□	□	□	資通安全政策或資通安全維護計畫
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	資通安全政策或資通安全維護計畫
	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？	□	□	□	審核紀錄及公告紀錄
	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？	□	□	□	管審會紀錄
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	公告紀錄
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？	□	□	□	資通安全組織成員表
	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？	□	□	□	資通安全組織成員表
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	資通安全組織成員表
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？	□	□	□	人員安全守則
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	資通安全維護計畫中敘明配置資通安全人員
	3.3 是否具備相關專業資安證照或認證？	□	□	□	專業安證照及職能訓練

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	3.4 是否配置適當之資源？	□	□	□	資安或資訊相關經費情形(全年度與前年度經費之占比)
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？	□	□	□	資訊資產清單
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資訊資產清單
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	維護計畫核心系統
	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？	□	□	□	資訊資產清單風險評估表
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？	□	□	□	資訊設備主機機房門禁照片
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	進出人員清單
	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？	□	□	□	人員進出紀錄表
	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？	□	□	□	巡查紀錄表
	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？	□	□	□	消防、CCTV、門禁設施檢查紀錄或保養資料。 設備使用訓練紀錄。
	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？	□	□	□	陪同進出之紀錄及照片
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	實體安全管理制度
	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？	□	□	□	例如：資訊機房偵煙、偵熱與滅火設備、漏水偵測等照片。
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	電力保護設施照片(UPS、穩壓器、接地線等)、緊急照明設備照片

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	線路保護設施照片(如線槽、高架地板、套管等)
	5.11 設備是否定期維護，以確保其可用性及完整性？	□	□	□	系統主機及網路維護紀錄或合約、機房查檢紀錄表
	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？	□	□	□	設備進出管理制度。(B-002 5.7.2) 設備進出紀錄表
	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)？	□	□	□	防毒軟體、登入等照片、設備領用紀錄。
	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？	□	□	□	報廢管理制度及報廢紀錄
	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？	□	□	□	管理制度及實體防護照片(例如：資料上鎖)。
	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？	□	□	□	測試環境與正式環境照片、不適用則免附。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	至少2位一般使用者的個人電腦設定畫面
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	至少2位一般使用者的個人電腦設定畫面
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	系統主機及個人電腦各兩臺設定畫面
	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)？	□	□	□	管理制度(B-007 5.3.5)
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	備份工作相關紀錄
	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？	□	□	□	備份回復演練紀錄
	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？	□	□	□	系統登作畫面、https、檔案加密。
	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	□	□	□	可攜式媒體管理制度

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	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？	□	□	□	帳號申請及註銷管理制度
	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？	□	□	□	帳號申請單及帳號清查表
	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)？	□	□	□	通行碼管理制度
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	通行碼管理制度
	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？	□	□	□	網路架構圖及業務與網段對應資料，內網區隔狀況、網路管理規定
	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？	□	□	□	遠端連線作業
	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)？	□	□	□	行動式電腦設備管理制度
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	憑證使用認證佐證資料 (不適用者免附)
	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？	□	□	□	資訊服務變更管理制度及紀錄。
	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？	□	□	□	弱掃報告及高風險弱點修補處理狀況
	5.35 限制使用危害國家資通安全產品	□	□	□	檢視資通系統及設備是否使用危害國家資通安全產品(如大陸品牌)
6.訂定資通安全事件通報及應變之程序及機制	6.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	資通安全事件通報及應變管理程序。
	6.2 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？	□	□	□	宣導及公告相關資料。

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	6.3 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？	□	□	□	安全事件報告單或矯正紀錄
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？	□	□	□	資通安全公告、宣導及研習資料
	7.2 是否對同仁進行資安評量？	□	□	□	資安評量或資安研習評量資料
	7.3 是否對同仁依層級定期舉辦資通安全教育訓練？	□	□	□	資安教育訓練資料 資通安全認知訓練時數要求： 1.全體同仁每人每年須接受3小時以上一般資通安全教育訓練。 2.專職(責)人員以外之資訊人員每人每年須接受3小時以上之資通安全專業課程訓練或資通安全職能訓練。 3.專職(責)人員每年須接受12小時以上資通安全專業課程訓練或資通安全職能訓練。
	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？	□	□	□	公告、宣導、人員安全守責等資料。
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	□	□	□	內稽制度
	8.2 是否定有年度稽核計畫？	□	□	□	內稽計畫書
	8.3 是否定期執行稽核？	□	□	□	內稽紀錄
	8.4 是否改正稽核之缺失？	□	□	□	內稽缺失矯正紀錄
9.資通安全維護計畫及實施情形之績效管考機制	9.1 是否訂定安全維護計畫持續改善機制？	□	□	□	矯正及預防管理制度
	9.2 是否追蹤過去缺失之改善情形？	□	□	□	矯正及預防處理單
	9.3 是否定期召開持續改善之管理審查會議？	□	□	□	管審會議紀錄
10.資通系統委外(含委辦)案之履約檢核及督導管理(無則請填寫不適用)	10.1 資通系統委外(含委辦)是否簽訂協議書或契約？	□	□	□	委外(含委辦)案之協議書、契約書等文件
	10.2 是否落實檢核及履約督導管理？	□	□	□	檢核受託單位繳交之資料(如弱點掃描報告陳核之證明文件)
	10.3 委外(含委辦)相關人員是否簽	□	□	□	保密切結書、保密合約書等文

查核項目	查核內容	查核結果			準備資料或客觀證據
		符合	不符合	不適用	
	訂保密合約書？				件
11.其他應辦事項	11.1 是否每年檢視一次資通系統(自有及委外)分級妥適性？	□	□	□	資通系統(自有及委外)分級相關文件(資通安全責任等級分級辦法附表九)
	11.2 是否配置一名資通安全專責人員？	□	□	□	資通安全專責人員報到紀錄或資安人員負責業務文件
	11.3 是否每兩年辦理一次資通安全健診？	□	□	□	資通安全健診報告
	11.4 是否完成資通安全防護(防毒軟體、網路防火牆、電子郵件過濾機制)？	□	□	□	1. 檢視資通設備是否安裝防毒軟體 2. 檢視網路防火牆建置情形 3. 具有電子郵件伺服器者，檢視電子郵件過濾機制

備註1:核心資訊系統須進行本表各個項目查核。

備註2:本表參考行政院資通安全會報之資通安全維護計畫制定。