內部稽核項目紀錄表					
文件編號	TWVS-ISMS-D-039	機密等級	一般	版次	3.0

查核依據：資安法與子法、主管機關函令、資安維護計畫與附件
查核範圍：全機關
查核日期：_____年_____月____日
查核人員：_____

查核項目	查核內容	查核結果			現場稽核 預估查檢方式 (實際稽核不以此為限)	稽核員記載發現
		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？	□	□	□	資安政策與目標適切性、核定、宣導、定期檢討等	
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	查閱管審會紀錄	
	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？	□	□	□	1.核准紀錄及宣導紀錄 2.傳達至機關人員之方式及有效性, ex.抽訪人員	
	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？	□	□	□	1.應訂定資通安全目標，設定量化與質性指標 2.績效指標訂定適切性、可行性 3.定期監控、量測、分析及檢視之方式(何時、方式、依據資訊) 4.檢視佐證資料：績效指標、定期檢視紀錄	
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	查閱公告紀錄，chk資安政策法令異動、資安新聞、教育訓練、資安事件學習等。	
2.設置資通安	2.1 是否指定適當權責之高階主	□	□	□	1.查閱資安組織表。	

全推動組織	管負責資通安全管理之協調、推動及督導等事項？				2.查核主管出席會議、訓練等資安業務情形。	
	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？	□	□	□	1.查閱資安組織表。 2.chk指派授權紀錄。	
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	1.查閱資安組織表。 2.chk人員職責、專業。	
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？	□	□	□	1.查閱人員資通安全作業相關文件，如人員資安管理手冊，說明人員資安注意事項，如人員進出規定、設備攜出入規定、個人電腦使用規定、電子郵件使用規定、網路使用規定等 2.了解保密協議及簽署紀錄(人員包括正式人員、約聘雇人員、委外人員等)。 3.若有符合狀況(事件)，追稽對當責人員的獎懲。	
	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資通安全專業人員。	
	3.3 是否具備相關專業資安證照或認證？	□	□	□	1.資通安全專業證照，指由主管機關認可之國內外發證機關(構)所核發之資通安全證照 2.依據資安處公告之資通安全專業證照清單 3.了解證書維護方式、證書有效性 4.取得證照者與專職(責)人員之關聯性 5.檢視佐證資料：證照證明、人員職責分	

					工表	
	3.4 是否配置適當之資源？	□	□	□	查閱 1.資安經費占資訊經費比例 2.資訊經費占機關經費比例 3.資安經費編列是否符合業務需要 4.資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查 5.檢視佐證資料：資安需求評估紀錄、年度預算規劃計畫、年度預算審核紀錄 Ex.資安經費佔比現況與趨勢，包括校預(決)算與外部經費，追近2~3年)	
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？	□	□	□	1.查閱資訊資產管理規章 2.資產類別(例如資訊資產、軟體資產、實體資產、支援服務資產等) 2.盤點範圍(全機關) 3.盤點方式(完整性) 4.資產清冊，如資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級 5.資產價值鑑別分級方式(CIA 或其他)、鑑別結果適切性 6.檢視佐證資料：資產清冊、資產價值鑑別紀錄 Ex.記載ex.數量、規格	
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	同上	
	4.3 是否定有資訊、資通系統分級	□	□	□	查核	

	與處理之相關規範？				1. 分級依據與規章 2. 系統分級討論核准紀錄	
	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？	□	□	□	查核 1.了解風險評估準則、衝擊準則及風險接受準則等風險管理基本準則 2.風險評估成員宜包含施政業務與支援該業務之資通系統相關人員，不宜只交由資訊或資安人員負責，以避免產出結果過於主觀，不符合該機關的真實現況 3.抽樣檢視風險評估適切性 4.風險處理程序 5.安控措施選擇、權責人員 6.風險處理計畫、安控措施、時程、權責人員等 7.風險處理計畫追蹤方式、處理情形 8.對於剩餘風險之處理 9.檢視佐證資料：程序文件、風險評估結果、風險處理措施及時程規劃、改善追蹤	
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？	□	□	□	查核 1.實體安全安控措施及規範 2.辦公環境及機房實體隔離 3.機房環境、動線、雜物、監視設備及有效性 4.檢視佐證資料：實體安全規範、門禁管理紀錄、相關申請紀錄	
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	查核 機房門禁進出控制措施授權定期清查紀錄。	1.

	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？	□	□	□	查核 1.人員進出紀錄表 2.依規則陪同或監視的紀錄，如cctv影像？	
	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？	□	□	□	查核 人工巡查紀錄? 或環控系統或運作與通報紀錄？	
	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？	□	□	□	查核 1.消防、CCTV、門禁設施檢查紀錄或保養資料。 2.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？	□	□	□	1.陪同進出之紀錄 2.抽查CCTV紀錄	
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	1.實體安全管理制度 2.抽查機房或業務區落實性	
	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？	□	□	□	查核： 1.設備實體環境控制安全，包括辦公地點、機房、發電機、UPS 等 2.機房之環境控制 3.機房之空調、電力備援 4.機房安全偵測及防護措施 6.chk佐證：檢查紀錄。	
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	查核電力與備援設施的配置、維護紀錄，包括 UPS、穩壓器、接地線、緊急照明設備等。	
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	抽查現場線路保護設施的保護情形，如線槽、高架地板、套管、接線標示等	

	5.11 設備是否定期維護，以確保其可用性及完整性？	□	□	□	抽查主機與支援設備及網路維護紀錄或合約、機房查檢紀錄	
	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？	□	□	□	1.查閱管理規章：設備進出。 2.抽查設備進出作業紀錄。	
	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)？	□	□	□	抽查 1.個人行動裝置攜入之安全要求、連網限制、存取限制 2.定期審查、監控紀錄。	
	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？	□	□	□	1.查閱報廢管理規章 2.抽查報廢作業紀錄 3.抽查現場。	
	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？	□	□	□	1.查閱管理規章。 2.抽查實地現場桌面淨空、資料上鎖、隨身碟、備份。	
	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？	□	□	□	若有自行開發系統，查核開發作業的測試環境與正式環境與作業紀錄。	
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	抽查人員電腦。	
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	抽查人員電腦。	
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	抽查人員電腦。	
	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)？	□	□	□	1.查閱管理規章。 2.抽查人員電腦作業。	
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	1.查閱管理規章。 2.抽查備份資料	

					3.抽查定期檢視備份紀錄	
	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？	□	□	□	1.檢視回復測試程序(如頻率、方式、測試環境等)及相關紀錄 2. 依回復測試情形或結果，定期檢視及修正復原程序 3. 檢視佐證資料：回復測試程序及相關紀錄、修正改善紀錄	
	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？	□	□	□	1.查閱管理規章。 2.抽查人員電腦作業，如系統登入、傳送機敏資料網頁(https)、傳送個資作業(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)管理程序？	□	□	□	1.可攜式媒體使用限制、存取控管、安全管理等 2.定期審查、監控紀錄 3.抽查人員實際作業。	
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	1.帳號申請及註銷管理制度 2.抽稽新到、異動、離職人員在各項設備的帳號。	
	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？	□	□	□	1.帳號申請單及帳號清查表 2.抽稽比對設備實際帳號與異動紀錄。	
	5.27 通行碼長度是否超過8個字元？	□	□	□	1.查閱管理規章。 2.抽查人員電腦作業。	
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	1.查閱管理規章。 2.抽查人員電腦作業。	
	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？	□	□	□	1.查閱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。 2.現場測試。	

	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？	□	□	□	1.查閱遠端連線作業規章。 2.抽查機器設定。 3.抽查異動作業紀錄。	
	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)？	□	□	□	1.查閱行動式設備規章 2.抽查NB與作業紀錄。	
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	查閱憑證使用認證制度與紀錄。	
	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？	□	□	□	1.查閱資訊服務／系統變更管理之檢查規章。 2. chk 檢查紀錄。	
	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？	□	□	□	1.弱掃報告，中高風險的系統與數量。 2.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-大陸廠牌產品清冊列管及說明。	□	□	□	1. 資通系統及設備清單 2. 現場檢核有無列管設備。	
	5.36限制使用危害國家資通安全產品-汰換大陸廠牌產品及說明。 1.110年12月31日前完成汰換大陸廠牌產品 2.如無法於期限內完成汰換，須於大陸 廠牌產品清冊述明理由。	□	□	□	如有 1. 汰換規劃紀錄。 2. 暫時無法汰換申請或核准紀錄。	
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？	□	□	□	查閱資通安全事件通報及應變管理程序。 1.知悉資通安全事件後，應於1小時內依主管機關關指定之方式及對象，進行資通安	

	資通安全事件通報及應變辦法第4 條：應於1小時內進行通報 *資通安全事件通報及應變辦法第9 條:應就資通安全事件之通報訂定作業規範*				全事件之通報。 2.應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： (1)判定事件等級之流程及權責 (2)事件之影響範圍、損害程度及機關因應能力之評估 (3)資通安全事件之內部通報流程 (4)通知受資通安全事件影響之其他機關之方式 (5)前四款事項之演練 (6)資通安全事件通報窗口及聯繫方式 3.應就資通安全事件之應變訂定作業規範，其內容應包括下列事項： (1)應變小組之組織 (2)事件發生前之演練作業 (3)事件發生時之損害控制機制 (4)事件發生後之復原、鑑識、調查及改善機制 (5)事件相關紀錄之保全 3.檢視佐證資料：資安事件通報應變作業規範、規範內容之落實紀錄	
	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？	□	□	□	抽查 1.宣導及公告紀錄。 2.抽稽人員知悉情形，含校內教職員工與委外廠商。	
	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？	□	□	□	抽查 1.近年資通安全事件內容 2.若同性質是建重覆發生，了解原因及改善追蹤落實	

					3.預防作業 4.檢視佐證資料：資安事件處理紀錄	
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？	□	□	□	查核 1.資安訓練主題適切性？ 2.學校與教育體系資安事件的再教育？ 3.訓練涵蓋人員？ 4.訓練有效性？	
	7.2 是否對同仁進行資安評量？	□	□	□	1.資安評量或資安研習評量資料 2.題目內容適切性？	
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	□	□	□	查核各種人員的資安教育訓練時數與有效性證明。 備註： *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？	□	□	□	抽查人員，確認對資安政策、目標、應負責任的了解程度。	
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？	□	□	□	抽查 1.內稽程序文件及稽核計畫(包括內稽頻率、時程、準則、檢核項目、方式、範圍等)，計畫書有明確執行的人事時地物說明。	

					2.稽核人員適切性、獨立性、勝任度等，ex.資格、迴避事項	
	8.3 是否定期執行稽核？	□	□	□	抽查內稽查核、報告等紀錄，確認有效與落實情形。	
	8.4 是否改正稽核之缺失？	□	□	□	抽查 最近2次內稽實際檢視改善情形，以及久未結案的原因。	
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？	□	□	□	查閱矯正及預防管理制度	
	9.2 是否追蹤過去缺失之改善情形？	□	□	□	抽查矯正及預防處理單或其他追蹤紀錄	
	9.3 是否定期召開持續改善之管理審查會議？	□	□	□	抽查近兩次以上管審會議紀錄	1.
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？	□	□	□	抽查委外資訊服務(所有含建置、保固、維運)的契約相關文件須符合： 1.資安法施行細則第四條的受託者應具備與應提供事項。 2.委外系統建置或維護合約明列系統防護基準。	1.
	10.2 是否落實檢核及履約督導管理？	□	□	□	抽查委外資訊服務(所有含建置、保固、維運)的檢核或督導管理証明，如： 1. 系統之定期(如週、季、月)或期中、期末系統營運、組態狀況、安全(如弱點掃描，廠商自辦內外稽報告)等項目報告。 2. 督導管理的紀錄。	
	10.3 委外(含委辦)相關人員是否簽訂保密合約書？	□	□	□	抽查委外資訊服務(所有含建置、保固、維運、顧問、稽核)的人員保密切結書、保密合約書等規定文件。	

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？	□	□	□	管理審查會議針對所有資訊系統之討論與決議紀錄。	
	11.2 是否每兩年辦理一次資通安全健診？	□	□	□	抽查 1資安健診近2次檢測時間、檢測方式、內容、結果 2.比較近2次結果，相同弱點存在時，可探其內容及原因，改善追蹤機制及落實情形 3.檢視佐證資料：檢測／複測報告、改善計畫、追蹤改善紀錄	
	11.3 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 4. 相關防護措施之防護規則、判斷原則及運作方式 ex, 電子郵件過濾原則、發現異常行為之因應 5. 檢視佐證資料：資通安全防護要求之相關作業程序、執行與查核紀錄	

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。

稽核結果：不符合項目：_____項