

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

紀錄編號：_____

填表日期： 年 月 日

評分標準說明：

- A：相關資訊安全管理制度規範已建立，且落實執行
- B：相關資訊安全管理制度規範未建立，但已實施替代性資安控管措施
- C：相關資訊安全管理制度規範已建立，但未落實執行
- D：相關資訊安全管理制度規範未建立，且未實施替代性資安控管措施
- E：不適用

稽核項目 - 規範本文

條款 章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
陸、	關於適用性聲明(Statement of Applicability)						
	本標準之設計為適用於教育體系與相關單位，但鑑於類型、規模、資源、業務性質等因素，若本標準列出之任何條款無法適用於某單位時，可考慮予以排除，但必須在不影響該單位提供資訊安全能力與責任之情況下，並提出理由。在建置完該單位之 ISMS 後，必須提出符合的適用性聲明，其中應包含選擇之控制目標與控制措施項目與理由，以及排除條款之內容、理由，作為稽核時的依據。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表

文件編號	NTSS-D-039	機密等級	限閱	版本	2.0
------	------------	------	----	----	-----

條款 章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
捌、	關於資訊安全管理系統 (ISMS)建置步驟						
捌、三	ISMS 之建立：依據該單位之類型、規模、資源、業務性質等特性，定義 ISMS 之範圍；考慮相關法律、法規，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之 ISMS 政策，並擬定一份適用性聲明書文件。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
捌、四	ISMS 之實施與操作：施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
捌、五	ISMS 之監控及審查：施行單位應針對 ISMS 進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查 ISMS 之有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
捌、六	ISMS 之維持及改進：施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
玖、	關於資訊安全管理系統 (ISMS)建置需求						
玖、七	文件要求：關於 ISMS 文件化（電子檔案或紙本），必須包含安全政策、安全目標、ISMS 範圍、適用性聲明、資安事件記錄，以及其他有助於提升 ISMS 成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
玖、八	管理階層責任：施行單位之管理階層，最為重要的是給予承諾及實際的支持，並適度的提供資源以助 ISMS 程序的進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於 ISMS 範圍內之員工，具備足夠之能力及認知，並定期進行教育訓練。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
玖、九	管理階層審查：管理階層應在規劃期間內，審查該單位的 ISMS 與適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
玖、十	ISMS 之改進：ISMS 的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

稽核項目 - 控制目標與控制項目

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A5	資訊安全政策訂定與評估							
A.5.1	資訊安全政策訂定與評估							
A.5.1.1	資訊安全政策制定	資訊安全政策應參考資安相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.5.1.2	資訊安全政策評估	面對資安事件的發生、資安相關法令與其他影響因素的改變時，資訊安全政策應進行即時的評估，並定期審查政策的可行性與有效性。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A6	資訊安全組織							
A.6.1	資訊安全組織推動與權責							
A.6.1.1	資訊安全組織推動以及權責之分配	由管理階層舉辦定期之資訊安全會報，召集相關單位代表進行工作與責任的分屬，確保資安相關計畫的進行，並展現管理階層的支持。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.6.1.2	資訊設施使用之授權	資訊處理設備的移轉（包含新設備），應由權責主管人員進行授權、移交的程序，確保該設備後續的順利運作及責任所屬。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.6.1.3	保密條款之 簽訂	施行單位之員工（包含正職員工、臨時雇員）應簽署獨立或包含保密條款之合約，確保其了解應有之資安責任與相關限制。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.6.1.4	跨單位合作 及協調	為確保資訊安全作業的順利運行，需與執法機關、主管機構、資訊服務廠商及電信公司建立適當的溝通管道。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.6.1.5	資訊安全諮 詢與顧問	在必要時，須向單位內部專業人員或外部專業諮詢人員徵詢、協調資訊安全建議。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.6.1.6	資訊安全政 策的獨立檢 視	機關制訂之資訊安全政策，應進行獨立及客觀的評估。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.6.2	施行單位外部人員存取安全管理							
A.6.2.1	施行單位外 部人員存取 之安全掌控	面對外部人員存取施行單位資訊處理設施的可能風險，應視狀況採取適當的安全控制措施，並條列安全規定於正式合約中。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.7	資訊資產分類與管制							
A.7.1	資訊資產分類與責任分屬							
A.7.1.1	資訊資產目 錄建立	應製作所有資訊資產之清冊，並定期維護、更新。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.7.1.2	資訊安全等 級分類	資訊資產應進行分級與標示，並考量重要資產的需求，於必要時制定保護措施及處理流程。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.8	人員安全管理與教育訓練							
A.8.1	聘任前之處理							
A.8.1.1	所屬角色與 責任	施行單位之員工、廠商及第三方使用者的資訊安全角色及責任應適需求以書面或其他方式清楚定義，並與資訊安全政策一致。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.8.2	聘用中之處理							
A.8.2.1	資訊安全教 育訓練	施行單位內所有員工、合作廠商與第三方使用者應接受適當之資安訓練與有關資安政策、程序之宣導課程。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.8.2.2	違反規定之 處理	依據既定之條款或合約，違反施行單位之資訊安全政策與程序之人員，應予以適當之懲處。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.8.3	結束聘任或改變職務							
A.8.3.1	結束聘用之 處理	負責執行結束聘用或改變職務之權責，其職掌應清楚定義並指派。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.8.3.2	資產繳回	離職時，應有正式的資產繳回程序，顯示其已繳回單位資產。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.8.3.3	存取權移除	所有員工、合約商及第三方使用者的存取權限應根據既有的規範或協定進行移除或改變。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9	實體與環境安全							
A.9.1	區域之安全							

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.9.1.1	實體環境安全	施行單位應採用適當防護措施保障資訊處理設施所在區域(機房設備、人員辦公區域)的安全。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.1.2	人員進出控制	施行單位應實施控制措施,確保只有授權人員可以進出安全區域。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.1.3	資訊處理設施安全	在資訊處理設施所在區域工作,應採取適當的控制措施與指引,確保該區域的安全性。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.2	設備之安全							
A.9.2.1	設備安置地點之保護措施	施行單位應安置或保護設備,降低環境之威脅、災害,以及未授權存取所造成的可能損失。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.2.2	電源供應	施行單位應保護資訊處理設備,降低電力故障或異常的影響。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.2.3	電纜線安全防護	施行單位應保護通訊纜線及資訊處理設備之電源,降低受竊聽或破壞的可能損失。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.9.2.4	設備之維護	資訊處理設備應予以適當的維護,確保其持續運作。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.2.5	設備報廢與再使用	資訊處理設備在報廢或再使用的過程中,應避免內存資料的外洩,進行必要之清除動作。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.9.2.6	預防未經授權之移動	施行單位所屬之設備、資訊或軟體未經授權禁止移動。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10	通訊與作業安全管理							
A.10.1	作業程序與責任							
A.10.1.1	作業程序文件化	安全政策所規定之作業程序，應文件化並定期維護。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.1.2	作業變更之管理	資訊處理設施、系統之變更，應進行管制。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.1.3	資訊安全責任之分散	職務與責任範圍需予區分，降低資訊或服務遭未授權修改或誤用之機會。 <i>—較適用於第一群</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.10.1.4	系統發展、測試及實務作業之分散	開發或測試用之設備、軟體轉換至作業狀態，應制定規則分隔開來，並加以文件化。 <i>—較適用於第一群</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.10.2	資訊作業委外服務之安全管理							
A.10.2.1	資訊作業服務之管控	施行單位執行資訊業務委外時，應與廠商簽訂適當的資訊安全協定及課予相關的安全管理責任，納入契約條款。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.2.2	服務之監控與審查	施行單位應監視和審查廠商提供的服務，確保服務標準達到協議的要求。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.2.3	廠商服務異動	面對廠商服務異動的管理程序，應注意相關的系統及程序，確實的掌控以避免導致新資安危機。 <i>—較適用於第一群</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.3	系統規劃與驗收							
A.10.3.1	系統作業容量之規劃	施行單位應適時預估系統容量需求，確保有充分處理資料與儲存的空間。 <i>—較適用於第一群</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.10.3.2	新系統上線作業之安全評估	新資訊系統、系統升級與新版本正式上線前應予以適當的測試，建立固定的驗收程序。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.4	電腦病毒、惡意軟體							
A.10.4.1	電腦病毒及惡意軟體之控制	施行單位應進行防備電腦病毒與惡意軟體之偵測及預防的控制措施，以及使用者認知程序。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.5	備份作業之管控							
A.10.5.1	資料備份	重要資訊與軟體應進行定期的備份。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.6	網路安全管理 <i>—較適用於學術網路系統</i>							
A.10.6.1	網路安全規劃與管理	應實施網路控制措施，維護網路安全。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.6.2	網路服務之 安全控制	使用公用或私用網路，應評估網路服務提供者之安全措施是否足夠，並提供明確的安全措施說明，另應考量使用該項網路對維持機關資料傳輸機密性、資料完整性及可用性各種安全影響。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.7	儲存媒體的處理與安全							
A.10.7.1	電腦媒體之 安全管理	電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.7.2	電腦媒體處 理之安全	應訂定電腦媒體的處理作業程序，以降低可能的安全風險。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.7.3	資料檔案之 保護	重要資料檔案應進行控管，並安全的保存。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.7.4	系統文件之 安全	重要系統文件應受到保護，避免未授權之存取。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.8	資訊與軟體交換							
A.10.8.1	資訊與軟體 交換安全政 策與協定	單位間交換資訊與軟體的行為（具機密性或敏感性內容）應有安全保護措施及協議規範，必要時制定正式合約。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.8.2	電子郵件安 全管理	應制定電子郵件使用政策，並實施控制措施降低安全風險。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.8.3	電子辦公系 統安全	視需求應制定並實施控制措施，以管制和電子辦公系統有關之單位及安全風險。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.8.4	對外公告資訊之管理	對外公告資訊前應有正式授權程序，並避免未授權之竄改。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9	系統存取及應用之監督							
A.10.9.1	事件記錄	建立及製作例外事件及資訊安全事項的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9.2	系統使用之監控	為確保使用者只能執行授權範圍內的事項，應建立系統使用監督程序。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9.3	記錄的保護	單位應保護未授權的變更及防止記錄設備操作發生問題。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9.4	系統管理者與作業人員之記錄	應忠實紀錄系統管理者與作業人員之相關操作記錄。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9.5	系統錯誤事項之紀錄	系統發生錯誤之事項時，應予以忠實的記錄，並進行適當的處理程序。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.10.9.6	系統時鐘應予同步	應定期校正系統作業時間，維持系統稽核紀錄的正確性及可信度，最為事後法律上或是紀律處理上的重要依據。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11	存取控制安全							
A.11.1	使用者存取控制							

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.1.1	使用者註冊管理	應制定正式使用者註冊、註銷流程和條款，以供存取資訊系統及服務。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.1.2	系統存取特別權限管理	限制與控管特許權限的分配及使用方式。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.1.3	一般通行碼之控管	應建立使用者通行碼之管理制度。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.1.4	系統存取權限之評估	施行單位應定期審查使用者存取權限。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.2	使用者責任							
A.11.2.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.3	網路存取控制措施							
A.11.3.1	網路服務之限制	施行單位須清楚限定使用者只能直接存取准許使用之服務。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.3.2	遠端使用者身分鑑別	遠端連線使用者之存取需進行身分鑑別。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.3.3	診斷埠 (Diagnostic Ports) 存取控制	診斷埠的存取行為必須嚴密控管。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.3.4	網路分隔控制	網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.3.5	網路連線控制	使用者連線能力應視需求予以限制。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.3.6	網路路由控制	共享網路應有路由控制措施，確保電腦連線及資訊流依循應用系統之存取控管政策。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.4	作業系統存取控制							
A.11.4.1	系統登入程序	使用者存取電腦系統應經由安全的系統登入程序。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.4.2	使用者通行碼管理	應以安全有效的使用者通行碼管理系統鑑別使用者身份。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.4.3	系統公用程式管理	系統上公用程式的使用，應予限制並控管。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.4.4	連線作業時間之控制	必要時限制使用者在高風險應用系統的連線作業時間。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.5	應用系統的存取控制 —較適用於行政資訊系統							

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.5.1	資訊存取限制	依資訊存取規定，配予應用系統的使用者與業務需求相稱的資料存取及應用系統的使用權限。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.11.5.2	機密及敏感性系統之獨立作業	必要時對機密性及敏感性系統，考量建置獨立的或是專屬的電腦作業環境。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.6	行動式電腦作業與遠距工作管理 —較適用於第一群							
A.11.6.1	行動式電腦作業控制	必要時應針對行動式電腦設施制定適當的控制措施及政策。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.11.6.2	遠距工作管理	施行單位應制定遠距工作活動的政策、流程及標準，控管相關活動的進行。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12	系統開發與維護之安全							
A.12.1	系統安全要求 —較適用於行政資訊系統 —較適用於第一群							
A.12.1.1	安全需求分析及規格訂定	應詳述新系統或既有系統之各項控制措施要求。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.12.2	應用系統安全 —較適用於行政資訊系統							
A.12.2.1	資料輸入之 驗證	輸入應用系統之資料須確認其正確性與適當性。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.12.2.2	系統內部作 業處理之驗 證	系統需建立確認檢查機制，以偵知所處理資料的 塗改。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.12.2.3	訊息真確性 之鑑別	必要時應採用訊息鑑別機制，保護訊息內容的完 整性。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.2.4	資料輸出控 管	應用系統的資料輸出需經過確認，確保處理程序 的正確性與適當性。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.12.3	加密控制措施 —較適用於第一群							
A.12.3.1	資料加密	必須發展加密控制措施保護資訊之政策。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.3.2	憑證機構之 技術安全	以一套公認之標準、流程及方法為金鑰管理系統 之基礎，支援加密技術之運用。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.4	系統檔案安全							

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.12.4.1	作業軟體控制	需建立作業系統各個軟體實施的管制程序，避免軟體影響作業系統之完整。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.12.4.2	系統測試資料之保護	系統之測試資料須予以保護與控管。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.4.3	原始程式庫資源之存取控制	原始程式庫 (Source Library)的存取必須採取嚴格的控制措施，避免在存取原始程式庫的程序中，造成原始程式庫的損毀。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.5	開發與支援作業的控制 —較適用於第一群							
A.12.5.1	變更作業之控制程序	實施變更作業應依循嚴格的變更管制措施。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.5.2	作業系統變更之技術評估	應用系統必須有所變更時，需進行必要之技術審核及測試。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.5.3	套裝軟體變更限制	避免修改套裝軟體，有必要修改時需採取嚴格管制。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.5.4	資訊洩漏控制	預防施行單位資訊遭洩漏的危機，制定適當的控管措施。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.12.5.5	軟體委外開發	軟體之委外、使用需採取適當之管制及檢查。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.12.6	系統弱點管理 —較適用於第一群							
A.12.6.1	系統弱點控制	應及時取得有關針對系統弱點的資訊，並評估該弱點暴露的程度及所造成的可能危機。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.13	資訊安全事件之反應及處理							
A.13.1	資訊安全事件與弱點之通報							
A.13.1.1	資訊安全事件與弱點通報	資安事件需即刻進行通報。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.13.2	資訊安全事件之管理							
A.13.2.1	資安事件處理責任與程序建立	應建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理機關資訊安全事件。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.13.2.2	從資安事件中學習	監控並紀錄事件的過程與結果，必要時進行檢討會議，討論改善之事宜。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.13.2.3	資安事件證據之收集	電腦稽核軌跡及相關的證據，應以適當的方法保護。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.14	業務永續運作管理 —較適用於第一群							
A.14.1	永續運作管理之規劃 —較適用於第一群							
A.14.1.1	業務永續運作之規劃程序	施行單位應建立業務永續運作之程序及架構，鑑定測試及維護之優先順序，訂定與維護永續運作之計畫。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.14.1.2	永續運作計畫之測試及更新	永續運作計畫應進行測試與維護，確保該計畫的有效性。 —較適用於第一群	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	不適用
A.15	相關法規與施行單位政策之符合性							
A.15.1	法規之遵守							
A.15.1.1	適用法規之鑑別	蒐集相關法律條文（智慧財產權、資料隱私保護及其他相關法規）、管理規定及合約要求，了解與資訊處理設施、軟體系統的關係，並予以書面或其他方式留存。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.15.1.2	適用法規之遵循	需制定適當的流程與管制，保護重要紀錄，並確保遵守智慧財產權、個人資料保護及隱私等條文規範，防止資訊處理設施遭不當之使用。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.15.2	安全政策與技術符合性之檢驗							

資訊安全管理制度內部稽核表					
文件編號	NTSS-D-039	機密等級	限閱	版本	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.15.2.1	確保遵守安全政策與規範	確保單位內所有區域或作業流程皆定期審查及確保遵守安全政策及規範。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.15.2.2	資訊系統符合性審查	為確保資訊系統之運行符合既定之安全實施標準，應進行定期的審查，並予以書面或其他方式留存。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.15.3	系統稽核的考量							
A.15.3.1	系統稽核控制	為避免作業系統稽核造成系統中斷的危險，應進行審慎、一致的規劃；必要時可向外部專家顧問尋求協助。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A.15.3.2	系統稽核工具之保護	系統稽核之相關工具需建立適當的保護措施，並視需求設立備援及緊急應變方案。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

資訊安全組組員：_____

資訊安全組組長：_____