國立中興大學
個人資訊管理制度內部稽核底稿
（教版）

機密等級：□公開使用 □內部使用 ■內部限閱 □機密

文件編號： NCHU-PIMS-D-018	版　　次：1.0
紀錄編號：	填表日期　　年　月　日

條款章節	條文	符合度				說明與結果
		符合	不符合	建議	不適用	
柒、	建置步驟及需求					
一、	組織全景					
	(一)施行機關(構)或學校應依據相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等之決)，針對資通安全或個人資料安全之維護需求進行評估，並據此建立或調整資通安全與個人資料管理範圍與目標。	□	□	□	□	
	(二)施行機關(構)或學校應依據決議事項確認其關注方(利害相關團體)與要求事項，並留存文件化紀錄。	□	□	□	□	
	(三)上述事項之識別與分析應定期審查(每年至少一次)，或於施行機關(構)或學校遭遇重大變更、或有新增業務時重新檢視，並供管理審查時，評估管理系統及其適用範圍是否有調整之必要性。	□	□	□	□	
二、	領導作為					
	(一)領導及承諾 管理制度管理人或召集人應由施行機關(構)或學校之副首長以上擔任或指定，並藉由下列事項，展現對管理制度之領導與承諾： 1.建立或核定機關(構)或學校之管理政策與目標。 2.傳達管理制度要求事項之遵循與持續改善的承諾。	□	□	□	□	

	3.提供管理制度運行所需資源及人力。					
	(二)建立政策與目標 1.管理人或召集人應確保建立文件化的管理政策，並於機關(構)或學校內進行公告或傳達，同時依需要提供予利害相關團體。	☐	☐	☐	☐	
	2. 管理政策應包含符合機關(構)或學校之管理目的與目標、滿足管理制度要求事項與、以及持續改善之承諾。	☐	☐	☐	☐	
	3. 施行機關(構)或學校應依規劃期間或重大變更時，於透過管理審查管理活動評估管理政策與目標，並配合變更需求修訂政策與目標。	☐	☐	☐	☐	
	(三)單位角色、責任及權限 管理人或召集人應建立制度管理小組，依機關(構)或學校特性，指派人員並賦予其管理之責任與權限，以促進達成本規範之要求事項。	☐	☐	☐	☐	
	受指派人員應定期(每年至少一次)或於重大變更時向管理階層報告管理制度執行成效。ISMS 與 PIMS 所配置人員應依據附錄 A.6 資訊安全組織與附錄 B.2 個人資料管理組織派任。	☐	☐	☐	☐	
三、	規劃					
	(一)管理目標達成風險與機會之因應行動 為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應依規劃期間或重大變更時，評估管理目標異動與達成情形，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動之有效性。 PIMS 並應依附錄 B.4 個人資料之識別與風險管理要求執行。	☐	☐	☐	☐	
	(二)建立風險管理程序 應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級。資訊系統經鑑別後，其安全等級屬最高等級者，應執行風險評估、擬訂與執行風險管理措施；其安全等級非屬最高等級者，應衡酌其風險程度，以決定是否進行風險評估、擬訂與執行風險管理措施。	☐	☐	☐	☐	

	風險評鑑與處理流程建立應符合下列要求事項： 1.建立與維持風險準則 包含風險評鑑執行時機與方法，以及風險接受準則，以確保重複之風險評鑑能產生一致、有效及可比較之結果。	☐	☐	☐	☐	
	2.識別、分析並評估風險 (1)識別管理制度適用範圍內涉及資訊之機密性、完整性、可用性與適法性相關聯之風險與風險擁有者。	☐	☐	☐	☐	
	(2)所識別之風險可能導致之潛在後果與發生的實際可能性，並將所建立之風險準則與風險分析結果進行比較，訂定風險處理優先順序。能性，並將所建立之風險準則與風險分析結果進行比較，訂定風險處理優先順序。	☐	☐	☐	☐	
	3.選擇風險處理措施 考量風險評鑑結果，選擇適切之風險處理選項，並依選項決定所有必須實作之控制措施。	☐	☐	☐	☐	
	4.產生或評估適用性聲明書(資訊安全風險處理使用) 執行資訊安全風險評鑑時，應依據資訊資產分級結果重現檢視比較現有控制措施及附錄 A，確認未忽略必要之控制措施，並產生或評估適用性聲明書，包括附錄 A 之控制措施，且不論是否實作，提供納入或排除之理由。	☐	☐	☐	☐	
	5.制訂風險處理計畫並取得核准 制訂風險處理計畫，並取得風險擁有者對風險處理計畫之核准，以及對剩餘風險之接受。	☐	☐	☐	☐	
	(三)管理目標及其達成之規劃 施行機關(構)或學校應針對異動與未達成之管理目標，設定符合管理政策與策略之可量測指標，並保存管理目標之文件化資訊。	☐	☐	☐	☐	
	施行機關(構)或學校應對前述管理目標規劃因應行動，包含： 1.相關執行活動或事項。 2.所需配置之人員、預算、設備技術與程序表單等資源。 3.活動或事項負責人員。 4.活動或事項預計完成時間。 5.管理目標是否達成之評估方式。	☐	☐	☐	☐	

四、	支援					
	(一)資源 施行機關(構)或學校應依據管理目標達成規劃，提供建立、實行、維持及持續改善管理制度所需資源。	☐	☐	☐	☐	
	(二)能力 施行機關(構)或學校應採取下列措施： 1.指派受過適當教育訓練、具備證照或具有經驗人員，執行資通安全或個人資料管理相關任務；規劃培訓以強化人員能力時，應評估培訓之有效性。	☐	☐	☐	☐	
	2.有關人員能力訓練，ISMS 應參照附錄 A.7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求執行。	☐	☐	☐	☐	
	3.應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員勝任之證據。	☐	☐	☐	☐	
	(三)認知 應規劃人員認知宣導或訓練，讓所有人員知悉： 1.管理政策及目標， 2.管理程序與流程要求事項與人員責任， 3.未遵循要求可能產生對個人與單位的影響與衝擊，其包含但不限於懲處。	☐	☐	☐	☐	
	ISMS 應參照附錄 A .7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求進行說明。	☐	☐	☐	☐	
	(四)文件化資訊 1.管理制度文件應包括本規範要求之文件化資訊，及施行機關(構)或學校要求管理制度為達成其有效性之文件化資訊與作業紀錄。 其文件化資訊至少應包含： (1) 決議事項確認其關注方(利害相關團體)與要求事項 (2) 管理政策 (3) 管理目標 (4) 人員勝任之證據 (5) 管理制度執行證據	☐	☐	☐	☐	

	(6) 風險處理計畫與風險處理結果 (7) 有效性評估證據 (8) 管理審查執行之證據 (9) 不符合項目及矯正措施					
	2.制訂及更新應遵循既有文件管理程序，進行審查及核准。	☐	☐	☐	☐	
	3.管控文件化資訊派送、存取、檢索、使用、儲放與維護、變更管制、留存及屆期處置，並適切保護。	☐	☐	☐	☐	
	4. 施行機關(構)或學校應識別對管理制度規劃及運作必要之外部文件。	☐	☐	☐	☐	
五、	運作					
	(一)運作之規劃及控制 施行機關(構)或學校之管理制度運作應滿足下列要求： 1. 應依據管理制度各階文件，以及為達成管理目標所規劃之流程、程序與控制措施執行，並應保存執行證據。	☐	☐	☐	☐	
	2. ISMS 應依據所屬級別實作選定之附錄 A 控制措施，PIMS 則應實作附錄 B 訂定之控制措施。	☐	☐	☐	☐	
	3.應確保各項委外執行作業受到控制與管理，屬 ISMS 委外管理可連結附錄 A 之 A.15 供應者關係，PIMS 則依據附錄 B 之 B.12 委外管理執行。	☐	☐	☐	☐	
	(二)執行風險評鑑 1.施行機關(構)或學校依規劃期間(至少每年一次)、管理階層指示或發生重大變更後一個月內，應執行風險評鑑，確認管理制度各項風險加以識別，並保存風險評鑑執行紀錄。	☐	☐	☐	☐	
	2.PIMS 施行機關(構)或學校應分析可能造成當事人損失或困擾之個人資訊處理流程，由風險擁有者進行審查。	☐	☐	☐	☐	
	3.擬定風險處理計畫，並取得風險擁有者對其及剩餘風險之核准。	☐	☐	☐	☐	
	(三)實作風險處理 施行機關(構)或學校應實作風險處理計畫並保存風險處理結果之文件化證據資訊。	☐	☐	☐	☐	

六、	績效評估					
	(一)監督、量測、分析及評估 1. 施行機關(構)或學校應針對已施行之常態性作業流程或控制措施建立監督機制，如機房管理、網路管理作業審查等。	□	□	□	□	
	2. 對於該年度異動之管理目標，以及風險處理措施設定有效性量測指標，並界定明確計算方式與資料來源、量測人員、週期與時間點，以及分析及評估量測結果之人員、週期與時間點。	□	□	□	□	
	3.應留存文件化資訊，作為有效性評估證據。	□	□	□	□	
	(二)內部稽核 1.施行機關(構)或學校應定期(至少每年一次)或於重大變更後執行一次內部稽核，以確認機關(構)或學校與人員是否遵循本規範與機關(構)或學校管理程序要求，並有效實作及維持管理制度。	□	□	□	□	
	2.稽核程序應包括頻率、方法、職責、規劃要求事項及報告。稽核計畫應包含適用範圍內核心業務與高風險個人資料流程或系統，並將前次稽核之結果納入考量。	□	□	□	□	
	3.稽核員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性。	□	□	□	□	
	4.稽核結果應對相關管理階層報告，留存相關紀錄以作為稽核計畫及稽核結果之證據。	□	□	□	□	
	(三)管理審查 管理小組應定期(每年至少一次)進行管理審查，以審查管理制度執行狀況，並確保其持續的適切性、合宜性及有效性。	□	□	□	□	
	1. 管理審查應包含下列討論事項： (1) 過往管理審查之議案的處理狀態 (2) 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項 (3) 管理目標與指標量測結果 (4) 內外部稽核結果 (5) 資安事故與不符合項目之矯正情形	□	□	□	□	

	(6) 風險評鑑結果及風險處理計畫執行進度 (7) 持續改善之機會					
	2.管理審查決議事項應包含持續改善機會與管理制度變更需求之決議。	☐	☐	☐	☐	
	3.施行機關(構)或學校應保存相關紀錄，以作為管理審查執行之證據。	☐	☐	☐	☐	
七、	改善					
	(一)不符合項目及矯正措施 不符合項目發生時，施行機關(構)或學校應進行下列作為，並保存紀錄： 1.先對不符合項目採取行動以控制並矯正，進而處理其後果。	☐	☐	☐	☐	
	2.判定其發生原因及矯正措施，並評估是否有其類似不符合項目存在，並據此提出並執行矯正措施，並必要時得考量對管理制度進行變更。	☐	☐	☐	☐	
	(二)持續改善 施行機關(構)或學校應持續改善管理制度的合宜性、適切性及有效性。	☐	☐	☐	☐	

國立中興大學
個人資訊管理制度內部稽核底稿
（教版）

機密等級：☐公開使用 ☐內部使用 ■內部限閱 ☐機密

文件編號：NCHU-PIMS-D-018	版　　次：1.0
紀錄編號：	填表日期　　年　月　日

款 章節	條文		符合度				說明與結果
			符合	不符合	建議	不用適	
B.1	個人資料管理政策						
B.1.1	個人資料管理方針						
B.1.1.1	個人資料管理政策	核准並定期審查個人資料管理政策，展現管理階層對遵循個人資料保護法律及良好實務的承諾					
		1.是否已訂定文件化之個人資料管理政策?	☐	☐	☐	☐	
		2.個人資料管理政策是否有經最高管理階層核定?	☐	☐	☐	☐	
		3.是否有採取任何的手段將個人資料管理政策傳達於所屬人員?	☐	☐	☐	☐	
		4.是否每年(每年至少一次)重新審查個人資料管理政策?	☐	☐	☐	☐	
		6.個人資料管理政策是否有包括下列資訊與承諾? (1) 僅基於施行單位合法目的下，進行必要的個人資料處理； (2) 僅針對特定目的蒐集最小化的個人資料，且不處理過多的個人資料； (3) 明確提供當事人其個人資料使用方式與對象的資訊；					

		(4) 僅處理相關且適當的個人資料； (5) 公平與合法的處理個人資料； (6) 維護個人資料分類清冊； (7) 保持個人資料的正確性，並依需要保持最新； (8) 僅依法律或施行單位合法目的的要求下，保存個人資料； (9) 尊重當事人行使其當事人權利； (10) 維護所有個人資料的安全； (11) 僅在受到適當保護下，將個人資料傳輸至我國境外； (12) 個人資料保護法律所允許之例外情形的應用； (13) 發展與實施 PIMS，使政策得以實施； (14) 適當時，鑑別內外部關注方，及其參與 PIMS 的程度； (15) 明確界定員工在 PIMS 中之責任與歸責性。 (16) 發展與實施 PIM 實施；					
B.2	個人資料管理組織						
B.2.1	內部組織						
B.2.1.1	管理階層角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循					
		1.是否有設置個人資料管理人?	☐	☐	☐	☐	
		2.個人資料管理人是否由校長、機構負責人擔任或指定?	☐	☐	☐	☐	
		3.個人資料管理人是否有負責督導安全維護計畫訂定及執行?	☐	☐	☐	☐	
		4.個人資料管理人之職責是否含括下列事項： (1) 核准個人資料管理相關政策；	☐	☐	☐	☐	

		(2) 依個人資料管理相關政策發展與實施PIMS； (3) 遵循個人資料管理相關政策執行安全與風險管理。					
B.2.1.2	日常作業管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	☐	☐	☐	☐	
		5. 個人資料管理人是否指定或設管理單位，或指定專人，負責個人資料檔案安全維護事項?	☐	☐	☐	☐	
		6.被指定負責個人資料檔案安全維護事項之專人是否具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作?	☐	☐	☐	☐	
		7.負責個人資料檔案安全維護事項之管理單位或專人是否有訂定及執行安全維護計畫，包括業務終止後個人資料處理方法?	☐	☐	☐	☐	
		8.負責個人資料檔案安全維護事項之管理單位或專人是否定期就個人資料檔案安全維護管理情形，向個人資料管理人提出書面報告?	☐	☐	☐	☐	
		9.負責個人資料檔案安全維護事項之管理單位或專人是否有依據稽核人員就計畫執行之評核，於進行檢討改進後，向個人資料管理人及稽核人員提出書面報告?	☐	☐	☐	☐	

		10.負責個人資料檔案安全維護事項之管理單位或專人所承担之日常作業政策遵循責任是否包括： (1) 發展與審核個人資料管理相關政策，並確保政策的實施。 (2) 政策的管理審查。 (3) 依政策要求，進行訓練與持續性認知宣導。 (4) 個人資料處理程序之核准? 。 (5) 協調組織內部風險管理與安全議題負責單位。 (6) 提供資料保護法令領域專家的意見與指引。 (7) 個人資料處理例外狀況的說明與應用。 (8) 提供資料分享方案相關建議(包含資料異地處理的安全議題) 。 (9) 蒐集與資料保護法令相關之法律修訂及合適的指導綱要。 (10) 持續確認法律、實務與科技的變化對 PIMS 帶來的改變。 (11) 考量任何具強制或諮詢性單位針對個人資料處理所制定之法規，經評估其適用性後於施行單位內實行。 (12) 持續評估施行單位遵循資料保護法令與最佳實務之狀況，並適時加以調整?	☐	☐	☐	☐	
		11. 個人資料管理人是否學校校長或機構負責人是否有指定個人資料稽核人員，以負責評核安全維護計畫執行情形及成效之人員。	☐	☐	☐	☐	
B.2.1.3	個人資料管理專人	建立各單位的個人資料管理窗口，協助個人資料相關日常作業的執行					
		12.若適用範圍涵蓋多個執行個人資料處理作業	☐	☐	☐	☐	

		的單位，各單位是否有指定專人擔任所屬單位的個人資料管理窗口?					
		13.前項之個人資料管理窗口是否有協助員工遵循個人資料管理相關政策並執行日常作業?	☐	☐	☐	☐	
B.3	人員認知與訓練						
B.3.1	個人資料管理認知與教育訓練						
B.3.1.1	政策認知訓練	透過政策認知訓練使個人資料管理成為核心價值與績效管理的一部分					
		1.是否定期或不定期對其所屬人員施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施?	☐	☐	☐	☐	
		2.是否有對對其所屬人員進行每年至少三小時的教育訓練或宣導，來提高、強化與維持對個人資料管理政策的認知?	☐	☐	☐	☐	
		3.是否建立並實行對其所屬人員個人資料管理政策認知評估方法，並留存評估紀錄?	☐	☐	☐	☐	
		4.是否透過各種可能管道，對其所屬人員傳達(1) 達成個人資料管理相關政策的目標，(2) 政策與作業流程的遵循，以及(3) 個人資料管理作業的持續改善的重要性?	☐	☐	☐	☐	
B.3.1.2	認知與教育訓練	透過訓練與宣導，使所有員工了解處理個人資料時應有的責任					
		5.為使被指定負責個人資料檔案安全維護事項之專人具有辦理安全維護事項之能力，是否有辦理或使專人接受相關專業之教育訓練?	☐	☐	☐	☐	
		6.個人資料管理相關人員是否對個人資料管理與保護相關法律與良好實務充分瞭解，並具有執行個人資料管理責任的能力?	☐	☐	☐	☐	
		7.個人資料管理相關人員是否知悉個人資料管理相關議題，並在適當時，透過與外部團體	☐	☐	☐	☐	

		接觸，讓員工持續獲得個人資料相關議題的訊息?					
		8.個人資料管理相關人員是否瞭解其應有的責任，使個人資訊處理能依據核定程序，並考量相關的安全要求，加以保護及處理?	☐	☐	☐	☐	
		9.個人資料管理相關人員是否能依適當程序處理個人資訊?	☐	☐	☐	☐	
		10.對個人資料管理相關人員之認知與教育訓練的內容是否有與其職掌及角色責任適當連結?	☐	☐	☐	☐	
B.4	個人資料之識別與風險管理						
B.4.1	個人資料之識別與維護						
B.4.1.1	個人資料清冊	清查並維護個人資料清冊					
		1.是否有確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，且每年至少清查一次所保有之個人資料現況?	☐	☐	☐	☐	
		2.清查之個人資料範圍是否包含施行單位蒐集、處理、利用、保存之所有個人資料，不論其取得來源，及留存於施行單位的期間?	☐	☐	☐	☐	
		3.是否有建立與維護個人資料清冊，且每年應至少更新一次?	☐	☐	☐	☐	
		4.個人資料清冊是否至少包括下列資訊：個人資料名稱、個人資料類別、特定目的、適用的法律規定與保存期限、個人資料流向?	☐	☐	☐	☐	
		5.是否依據「附錄 A 資訊安全管理規範」A.8 資訊資產管理，或機構機密資料等級要求，將高風險個人資料列入機密或敏感資料，並依據對應之機密等級進行標示與處置?	☐	☐	☐	☐	

B.4.1.2	高風險個人資料	應鑑別高風險個人資料					
		6.是否有依據業務特性界定高風險或敏感個人資料類別?	☐	☐	☐	☐	
		7.高風險或敏感個人資料之定義是否有包括個人資料保護法第六條所提及之個人資料(醫療、基因、性生活、健康檢查及犯罪前科)?	☐	☐	☐	☐	
B.4.2	個人資料之風險評鑑及管理						
B.4.2.1	風險評鑑	確保組織瞭解，特定類型個人資料處理時任何相關風險。					
		1.是否就已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施?	☐	☐	☐	☐	
		2.是否依據本規範柒、三規劃內所建議之風險評鑑與處理流程，與附件建議之風險評鑑方法來評估當事人因個人資料處理而可能面臨的風險等級?	☐	☐	☐	☐	
		3.委外執行的個人資料管理作業是否納入風險評鑑項目?	☐	☐	☐	☐	
		4.是否針對風險評鑑流程中所識別的各項風險，應進行風險處理作業，以降低違反政策要求的可能性?	☐	☐	☐	☐	
		5.是否有依據程序,將任何可能造成當事人損失或(及)困擾之個人資訊處理流程於管理審查活動中向個資管理人與個人資訊風險擁有者進行陳報與審查?	☐	☐	☐	☐	
B.5	公正與合法的處理						
B.5.1	蒐集與處理						
B.5.1.1	蒐集與處理作業審查	定期審查作業流程，以確保公正且合法的蒐集與處理個人資料					
		1. 是否有建立個人資料之蒐集、處理或利用之內部程序?	☐	☐	☐	☐	

		2. 於重大變更發生時，是否有針對與個人資料相關之蒐集與處理作業流程進行審查確認?	□	□	□	□	
B.5.2	告知與同意						
B.5.2.1	告知事項	告知事項應符合個人資料保護法令要求					
		1.施行單位如屬公務機關,其是否有依個人資料保護法要求在全球資訊網等官方網站上公開個人資料檔案相關資訊?	□	□	□	□	
		2.除有個人資料保護法第 8 條所定之免告知事由，依個人資料保護法第 15 條或第 19 條規定向當事人蒐集個人資料時，是否有明確告知事當事人下列事項? (13) 公務機關或非公務機關名稱。 (14) 蒐集之目的。 (15) 個人資料之類別。 (16) 個人資料利用之期間、地區、對象及方式。 (17) 當事人依第三條規定得行使之權利及方式。 (18) 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 *免告知事由： 一、依法律規定得免告知。 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。 三、告知將妨害公務機關執行法定職務。 四、告知將妨害第三人之重大利益。 五、當事人明知應告知之內容。	□	□	□	□	
B.5.2.2	告知或同意作業程序	訂定管理程序，以確保告知作業之執行及執行證據保存					

		3.依個人資料保護法第 8 條或第 9 條向當事人為告知時，其方式是否足以使當事人知悉或可得知悉法定告知事項內容?	☐	☐	☐	☐	
		4.告知事項是否完整?	☐	☐	☐	☐	
		5.如由其他外部單位蒐集或取得個人資料是否有確保公平與合法地蒐集個人資料?	☐	☐	☐	☐	
B.6	個人資料特定目的處理						
B.6.1	蒐集與處理特定目的						
B.6.1.1	特定目的處理準則	個人資料僅於特定目的下處理與使用					
		1.是否有訂定特定目的審查流程，以審查個人資料處理與利用情形，確保於處理個人資料的過程中，不會產生違反或潛在違反任何法定義務之情況，包含法令條文、一般法律或契約條款等?	☐	☐	☐	☐	
		2.是否有訂定特定目的審查流程，以確保除了有個人資料保護法第 16 條或第 20 條所定之情形外，個人資料不會用於個人資料蒐集之特定目的以外的目的?	☐	☐	☐	☐	
		3.個人資料之蒐集與處理是否具有特定目的，並符合個人資料保護法第 15 條或第 19 條之規定?(有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，應依個人資料保護法第 6 條規定為之，惟本規定現暫緩施行) *受查核機構如為公務機關應適用個人資料保護法第 15 條；如為非公務機關應適用個人資料保護法第 19 條規定。	☐	☐	☐	☐	
		4.如以經當事人書面同意之方式作為個人資料之蒐集與處理之依據，該書面同意是否為向當事人告知本法所定應告知事項後，由其所為允許之書面意思表示?	☐	☐	☐	☐	

B.6.1.2	新特定目的同意	個人資料用於新增特定目的應取得當事人書面同意	☐	☐	☐	☐	
		5.個人資料之利用是否合於個人資料蒐集之特定目的? 如不符合(即為特定目的外之利用)，是否合於個人資料保護法第 16 條或第 20 條所定之情形? *受查核機構如為公務機關應適用個人資料保護法第 16 條;如為非公務機關應適用個人資料保護法第 20 條規定。	☐	☐	☐	☐	
		6.如以經當事人書面同意之方式作為特定目的外之利用之依據，該書面同意是否為向當事人明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，由其單獨所為之書面意思表示?	☐	☐	☐	☐	
		7.取得當事人同意特定目的外之利用之書面意思表示，如係與其他意思表示於同一書面為之時，是有於適當位置使當事人得以知悉其內容並確認同意?	☐	☐	☐	☐	
		8.擬將個人資料用於新特定目的並須取得當事人書面同意時，是否有確定新特定目的的同意，是出於自由意識的執行與告知?	☐	☐	☐	☐	
		9.擬將個人資料用於新特定目的並須取得當事人書面同意時，是否有保存當事人獨立意思表示之書面同意記錄?	☐	☐	☐	☐	
		10.利用個人資料為宣傳、推廣或行銷時，是否明確告知當事人其所屬學校、機構立案名稱及個人資料來源?	☐	☐	☐	☐	
		11.首次利用個人資料為宣傳、推廣或行銷時，是否提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用?	☐	☐	☐	☐	

		12.當事人表示拒絕宣傳、推廣或行銷後，是否立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員?	☐	☐	☐	☐	
B.6.2	資料分享與揭露						
B.6.2.1	資料分享規劃與協議	資料分享應符合法令規範，簽訂資料分享協議取得合法使用承諾，並留存可供稽核紀錄					
		1.資料分享前是否與其分享個人資料之單位簽訂正式協議書或契約等正式文件?	☐	☐	☐	☐	
		2.前項協議書或契約是否有記載雙方於個人資料管理的責任?	☐	☐	☐	☐	
		3.前項協議書或契約是否說明個人資料使用的目的，並限制或禁止為其他目的進一步使用該個人資料?	☐	☐	☐	☐	
		4.是否有審查任何涉及將資料分享予第三方之新處理程序，於涉及新增的分享對象時，考量調整個人資料蒐集告知內容的必要性?	☐	☐	☐	☐	
		5.是否於確認在資料分享不違反法律規範及契約義務的前提下，必要時於分享前取得當事人的書面同意?	☐	☐	☐	☐	
		6.當資料分享符合個人資料保護法要求而不需取得當事人同意時，是否有考量留存可稽核的文件化紀錄?	☐	☐	☐	☐	
B.6.2.2	資料揭露程序	訂定管理程序，以確保僅於合法且必要情況下揭露個人資料					
		7.是否有拒絕揭露所蒐集、處理與保存的個人資料之無關第三人請求?	☐	☐	☐	☐	
		8.基於法令規定，是否僅於合法且必要的情境下(如：接獲法院命令)，向經驗證符合身分的有合法權限的機關或對象，揭露最小化的個人資料?	☐	☐	☐	☐	

		9.是否針對要求資料揭露的第三方,驗證其所宣稱的身分、存取個人資料權利及法源依據的真實性?	☐	☐	☐	☐	
		10.於可行時，是否僅揭露最少數量的個人資料予第三方?	☐	☐	☐	☐	
		11.是否留存資料揭露的作業紀錄，以追蹤個人資料揭露之軌跡，並包含其合法證明?	☐	☐	☐	☐	
B.6.3	資料比對						
B.6.3.1	資料比對	透過資料比對而產出的個人資料，應確保其比對作業及使用，符合特定目的或法律要求					
		1.於將不同來源或特定目的取得的個人資料,進行比對而產出的個人資料，如透過多筆間接識別個人資料比對以產生的直接識別個人資料，其使用是否符合特定目的或遵循相關法律要求?	☐	☐	☐	☐	
B.7	適當相關與正確性						
B.7.1	適當性相關且不過度						
B.7.1.1	適當性管理	個人資料的蒐集與使用的適當性審查					
		1.個人資料之蒐集、處理或利用是否有尊重當事人之權益，依誠實及信用方法為之，且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯?	☐	☐	☐	☐	
		2.是有建立每年審查個人資料蒐集與使用適當性之作業程序或方法?	☐	☐	☐	☐	
		3.是否所蒐集的個人資料,對特定目的而言是適當的?	☐	☐	☐	☐	
		4.是否個人資料的處理技術與流程得以確保個人資料蒐集與使用之適當性?	☐	☐	☐	☐	
		5.是否有建立每年重新審查一次所蒐集與使用的個人資料及相關作業流程之作業程序或方法?	☐	☐	☐	☐	

B.7.1.2	相關且不過度管理	個人資料的蒐集與使用相關且不過度審查					
		6.是否有建立每年重新審查一次所蒐集與使用的個人資料及相關作業流程之作業程序或方法?	☐	☐	☐	☐	
		7.是否僅在符合法令要求及特定目的要求下,處理最少量的個人資料?	☐	☐	☐	☐	
		8.是否有處理超出告知事項的額外個人資料,但卻未取得當事人書面同意?	☐	☐	☐	☐	
		9.涉及個人資料處理之新系統、流程或作業表單，是否有審查處理之個人資料是相關且不過度的?	☐	☐	☐	☐	
		10.於組織重大變更時，是否針對調整後的個人資料相關作業流程及表單進行審查，以確保其相關且不過度?	☐	☐	☐	☐	
B.7.2	個人資料正確性						
B. 7.2.1	正確性管理	整合個人資料的正確性管理至作業流程中					
		1.於設計或調整個人資料相關作業流程時,是否有考量個人資料正確性的維護與保護?	☐	☐	☐	☐	
		2. 是否有維護個人資料之正確?	☐	☐	☐	☐	
		3.是否主動或依當事人之請求,更正或補充個人資料?	☐	☐	☐	☐	
		4.除非因執行職務或業務所必須並註明其爭議或經當事人書面同意者，是否主動或依當事人之請求停止處理或利用正確性有爭議之個人資料?	☐	☐	☐	☐	
B. 7.2.2	錯誤資料的更正	應通知或更正提供予其他施行單位的個人資料的錯漏	☐	☐	☐	☐	
		5.因可歸責於公務機關或非公務機關之事由,未為更正或補充之個人資料，是否於更正或補充後，通知曾提供利用之對象?	☐	☐	☐	☐	

		6.知悉個人資料錯誤或非最新時,是否有通知資料分享的第三方，不可使用於影響當事人權益的決策?	☐	☐	☐	☐	
		7.知悉個人資料錯誤或非最新時,是否在符合個人資料保護法律要求或情況允許時，將正確之個人資料傳遞予第三方?	☐	☐	☐	☐	
B. 7.2.3	新流程的審查	審查新流程或系統,確保其可達成個人資料正確性的維持	☐	☐	☐	☐	
		8.是否有審查新增涉及處理個人資料的流程或系統，以確認其已盡可能避免記錄任何錯誤或過時的個人資料?	☐	☐	☐	☐	
		9.是否有審查新增涉及處理個人資料的流程或系統，以確認允許修正錯誤或過時的個人資訊?	☐	☐	☐	☐	
B.8	保存與處置						
B.8.1	保存與銷毀						
B.8.1.1	資料保存與銷毀程序	訂定管理程序，以確保個人資料保存與銷毀要求的落實					
		1.是否有訂定個人資料保存與銷毀管理相關程序，包括訂定紙本資料之銷毀程序在內?	☐	☐	☐	☐	
		2.是否根據單位及檔案屬性,相關法令及施行單位要求，訂定檔案保存要求與保存期限並經個人資料管理小組核可?	☐	☐	☐	☐	
		3.是否定期(至少每年一次)檢視其所保有個人資料之特定目的是否消失,或期限是否屆滿?	☐	☐	☐	☐	
		4. 確認特定目的消失或期限屆滿時而無保存必要者，是否有依個人資料保護法第十一條第三項規定進行刪除、銷毀或其他停止蒐集等適當之處置?	☐	☐	☐	☐	

		5.是否基於執行職務或業務所必須或經當事人書面同意，繼續處理或利用蒐集之特定目的消失或期限屆滿之個人資料? *執行職務或業務所必須： 一、有法令規定或契約約定之保存期限。 二、有理由足認刪除將侵害當事人值得保護之利益。 三、其他不能刪除之正當事由。	☐	☐	☐	☐	
		6.對於違反本法規定蒐集、處理或利用個人資料者，是否主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料?	☐	☐	☐	☐	
		7.個人資料銷毀作業之執行，是否遵循文件銷毀程序，並採用適合個人資料風險等級的安全措施，且留存文件化作業紀錄?	☐	☐	☐	☐	
		8.超過保存期限之個人資料，當基於正當理由暫不銷毀時，是否造冊列管?	☐	☐	☐	☐	
		9.前項清冊是否至少包含超過保存期限之個人資料明細、保存之正當理由，與預定銷毀期限或條件?	☐	☐	☐	☐	
		10.待銷毀資料是否依其風險程度受適宜保護?	☐	☐	☐	☐	
B.9	當事人權利						
B.9.1	當事人權利行使						
B.9.1.1	當事人權利行使程序	訂定管理程序，以確保當事人行使其法定權利					
		1.是否訂定當事人權利行使相關程序?	☐	☐	☐	☐	
		2.是否建立當事人權利行使聯絡窗口、聯絡方式，以及處理流程?	☐	☐	☐	☐	
		3.當事人權利行使流程是否涵蓋處理個人資料的所有單位，以個人資料管理小組為管理單位，並由各單位個人資料管理專人擔任單位連絡窗口?	☐	☐	☐	☐	

		4.是否已明定個人資料當事人可行使的權利及回覆時效? *個人資料保護法第 11 條 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。 公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。	☐	☐	☐	☐	
		5.是否已建立當事人個人權利行使申請、執行進度追蹤機制、及定期清查的流程?	☐	☐	☐	☐	
		6.受理當事人權利行使時,是否有確認為資料當事人之本人，或經其委託者?	☐	☐	☐	☐	
		7.是否有告知有無酌收必要成本費用及其收費基準?	☐	☐	☐	☐	
		8.如具有個人資料保護法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人行使權利之事由，回覆時是否有通知當事人並一併附理由通知當事人?	☐	☐	☐	☐	
		9.當事人個人權利行使是否留存可供稽核之執行紀錄?	☐	☐	☐	☐	
B.9.1.2	抱怨與申訴流程	受理並正確處理個人資料相關抱怨與申訴案件	☐	☐	☐	☐	
		10.是否有設計抱怨與申訴的受理處理流程，以確保有關個人資料處理之抱怨，得到正確的處理?	☐	☐	☐	☐	
		11.是否有接受當事人抱怨，與對抱怨處理方式提出申訴之窗口與流程?	☐	☐	☐	☐	

		12.是否每年至少清查一次當事人抱怨與申訴之處理進度與結果，並將清查結果納入持續改善之考量?	☐	☐	☐	☐	
B.10	資料安全議題						
B.10.1	安全控管措施						
B.10.1.1	個人資料控管措施	設定並審查個人資料蒐集、處理、儲存、傳輸與存取監控的安全控制措施或科技					
		1.是否就個人資料的蒐集、處理、儲存、傳輸與存取監控，明確設定安全控制措施或採取適當的科技保護措施?	☐	☐	☐	☐	
		2.個人資料控管措施是否有考量個人資料數量、類別、型態及外洩時對當事人造成的損失或困擾之風險?	☐	☐	☐	☐	
		3.安全控制措施是否與個人資料風險等級相當，如基於正當理由降低，應採取補償性控制措施?	☐	☐	☐	☐	
		4.是否有持續維護安全控制技術之正確性及功能適切性?	☐	☐	☐	☐	
		5.有關個人資料對內及對外傳輸,是否選用預先核准且符合個人資料風險等級的保全方式或科技，以防護傳送中的資料?	☐	☐	☐	☐	

		6.是否依據「附錄 A 資訊安全管理規範」中下列控制領域或目標之控制項要求進行存取權限管理? A.8 資產管理：個人資料處理、儲存與傳輸與其載體(如紙本、儲存媒體)之安全管理。 A.11 實體及環境安全：個人資料處理、儲存與傳輸設備置放環境與維護管理。 A.12 運作安全：個人資料處理設備日常管理、惡意軟體防治、備份、軌跡紀錄等管理。 A.13 通訊安全：個人資料傳送政策與書面協議，以及傳送安全管理。 A.14 系統獲取、開發及維護：涉及個人資料處理之資訊系統安全規格建立，測試要求，以及測試資料處理管理。	□	□	□	□	
		7.是否建立與落實紙本資料檔案之安全保護設施及管理程序?	□	□	□	□	
		8.電子資料檔案存放之電腦或自動化機器相關設備，是否配置安全防護系統或加密機制?	□	□	□	□	
		9. 是否訂定與落實紙本資料之銷毀程序?	□	□	□	□	
		10.電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，是否有採取適當防範措施，避免洩漏個人資料?	□	□	□	□	
		11. 是否依據「附錄 A 資訊安全管理規範」中下列控制領域或目標之控制項要求進行? A.6 資訊安全之組織：配合現有資訊安全管理組織，建立個人資料相關人員之角色與責任。 A.7 人力資源安全：個人資料流程相關人員之管理，確保個人資料處理人員的責任、認知訓練，以及責任終止後的義務。	□	□	□	□	

		12.是否依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性?	□	□	□	□	
		13.是否檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員?	□	□	□	□	
		14.是否要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務?	□	□	□	□	
		15.所屬人員離職時取消其識別碼，是否要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接，不得攜離使用，並簽訂保密切結書?	□	□	□	□	
		16.是否配合「附錄 A 資訊安全管理規範」中 A.8 資產管理與 A.11 實體及環境安全中對於個人資料媒體與設備之汰除與處理要求執行?	□	□	□	□	
		17.是否就業務終止後，就保有之個人資料之處理方式及留存紀錄，訂定相關程序? *個人資料之處理方式及留存紀錄如下： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 三、刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。	□	□	□	□	

		18.執行安全維護計畫各項程序及措施，是否有保存下列紀錄： 一、個人資料之交付及傳輸。 二、個人資料之維護、修正、刪除、銷毀及轉移。 三、提供當事人行使之權利。 四、存取個人資料系統之紀錄。 五、備份及還原之測試。 六、所屬人員權限之異動。 七、所屬人員違反權限之行為。 八、因應事故發生所採取之措施。 九、定期檢查處理個人資料之資訊系統。 十、教育訓練。 十一、安全維護計畫稽核及改善措施之執行。 十二、業務終止後處理紀錄。	☐	☐	☐	☐	
B.10.1.2	存取權限管理程序	以正式程序最小化授予並審查個人資料存取權限	☐	☐	☐	☐	
		19.是否依據個人資料盤點與風險評鑑結果，訂定個人資料處理權限?	☐	☐	☐	☐	
		20.個人資料之存取權限控制措施，是否符合其風險等級，尤其是特種個人資料?	☐	☐	☐	☐	
		21.所有個人資料的存取作業是否皆受到監控?	☐	☐	☐	☐	
B.10.1.3	安全控制措施審查	定期審查安全控制措施的有效性					
		22.是否有訂定個人資料檔案安全稽核機制，或配合資訊安全管理系統稽核機制，每年或於重大變更後檢查個人資料安全控管措施是否落實執行?	☐	☐	☐	☐	
		23.是否配合風險評鑑進行評估現行安全控制措施，以確保有使用合適的流程、方法、科技與設備，並於必要時提供改善建議?	☐	☐	☐	☐	

		24.是否配合風險評鑑進行評估現行安全控制措施，以確保該措施有考量當安全事故發生時，對當事人造成損失及困擾的風險?	☐	☐	☐	☐	
B.10.2	安全事故管理						
B.10.2.1	安全事故管理程序與紀錄	訂定管理程序，以妥善處理安全事故並留存可供後續追查的紀錄	☐	☐	☐	☐	
		1.是否有訂定與落實個人資料安全事故管理相關程序與應變機制，以確保在發生個人資料被竊取、洩露、竄改或其他侵害事故時，能夠迅速處理該事故並保護當事人之權益? *應變機制，應至少包括下列事項： 一、採取適當之措施，控制事故對當事人造成之損害。 二、查明事故發生原因及損害狀況，並以適當方式通知當事人。 三、研議改進措施，避免事故再度發生。	☐	☐	☐	☐	
		2. 是否有設置個資保護聯絡人員及重大個資事件單一通報與聯繫管道，將個資保護聯絡方式（如：電話、email）置於單位網站，以便利個資當事人提出申訴與救濟?	☐	☐	☐	☐	
		3. 是否有依據「附錄 A 資訊安全管理規範」中 A.16 資訊安全事故管理各控制項要求建立個人資料安全事故管理與應變機制?	☐	☐	☐	☐	
		4. 於查明事故發生原因及損害狀況後，是否以適當方式通知當事人個人資料被侵害之事實及已採取之因應措施?	☐	☐	☐	☐	

		5. 前項通知方式是否即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之? (*但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之)	☐	☐	☐	☐	
		6. 於發生安全事故時，是否有依據「政府機關（構）資安事件數位證據保全標準作業程序」或相關證據保全作業規範進行數位證據之蒐集與保存?	☐	☐	☐	☐	
B.11	國際傳輸						
B.11.1	國際傳輸管理						
B.11.1.1	境外管理協議與保護	傳輸至我國境外的個人資料應受到良好的管理					
		1.將個人資料傳輸至我國境外前，是否檢視中央目的事業主管機關有無依個人資料保護法第二十一條規定為限制國際傳輸之命令或處分，並遵循之?	☐	☐	☐	☐	
		2.將個人資料傳輸至我國境外前，是否簽訂書面協議或契約，以明訂管理責任，包含但不限於：個人資料傳輸與保存方式、使用與處理限制、資料銷毀要求等?	☐	☐	☐	☐	
		3.資料傳輸方式及資料接收單位，是否已採用與資料風險等級相符的資料保全流程、設施與科技，並經個人資料管理小組(B.2.1.2)審查核可?	☐	☐	☐	☐	
B.11.1.2	傳輸法令遵循	個人資料的傳輸應符合我國相關法律要求					
		4.個人資料傳輸至我國境外時，是否有確認傳輸行為、協議或契約，符合我國相關法律及教育部之規範?	☐	☐	☐	☐	
B.12	委外管理						
B.12.1	個人資料作業委外管理						

B.12.1.1	委外管理程序	篩選及管理委外機構					
		1.是否依據「附錄 A 資訊安全管理規範」中控制領域A.15供應者關係之所有控制項要求進行個人資料作業委外管理?	☐	☐	☐	☐	
		2.前項所稱之個人資料作業委外管理,其內容是否包含個人資料安全管理要求，且符合個人資料保護法施行細則第十二條安全維護事項之要求?	☐	☐	☐	☐	
		3.於個人資料委託其他單位進行處理前,是否執行受委託機構評選,並僅選與可達成科技面、實體面及組織面安全要求的機構進行合作?	☐	☐	☐	☐	
		4.於個人資料委託其他單位進行處理前,是否與受委託機構簽訂委託管理協議?	☐	☐	☐	☐	
		5.前項委託管理協議是否包含 B.12.1.2 委託協議要項與「附錄 A 資訊安全管理規範」A.15供應者關係中資訊安全要求事項?	☐	☐	☐	☐	
		6.是否有定期確認受託者執行之狀況,並將確認結果記錄之?	☐	☐	☐	☐	
B.12.1.2 (I/P)	委外協議要項	於協議載明委外要求，以管理委外機構					
		7.是否依個人資料保護法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式?	☐	☐	☐	☐	

		8.前項委託協議內容是否至少包含以下要求： (1) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (2) 受委託機關的保密及安全管理責任，及安全事故責任歸屬； (3) 委託機構得對其作業流程及安全控制措施進行稽核； (4) 是否被允許分包個人資料處理作業；如允許分包，分包機構應至少執行與委託協議同等的安全控制措施； (5) 受託機構或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機構通知之事項及採行之補救措施。 (6) 委託機構如對受託者有保留指示者，其保留指示之事項。 (7) 委託關係終止或解除時，個人資料載體之返還，及受委託機構履行委託契約以儲存方式而持有之個人資料之刪除。 (8) 其他我國個人資料保護法律要求的要項。	□	□	□	□	