附件1　個資保護管理建置流程檢核表

階段	編號	檢核項目	說明	是	部分	否	不適用	備註
規劃階段	1	個資管理組織架構	依據組織的需求與特性，規劃後續進行個資管理活動所需之功能性組織架構，以及架構中相關人員的角色職責，以利溝通協調運作。同時擬定組織的個資管理政策與要點，做為後續執行個資管理活動的最高指導原則。					
	2	外部環境分析	瞭解組織外部環境對於個資的相關需求，例如個資法與其施行細則、國際隱私保護原則及個資管理標準等，並識別與分析和組織間有個資往來活動之外部利害關係人，例如當事人、供應商、委外廠商或人員、合作組織及策略聯盟等。					
	3	內部環境分析	識別與分析組織內部現行和個資有關的管理制度內容、應用範圍、單位或人員等資訊。然後彙整個資內外部環境與利害關係人之分析結果，做為組織規劃與建置後續個資保護管理各階段範圍的參考。					

階段	編號	檢核項目	說明	是	部分	否	不適用	備註
	4	作業流程分析	依據組織所規劃後續各階段建置個資管理的範圍，進行相關服務目錄與服務等級協議、業務作業流程及委外作業流程的分析，以明確定義各階段範圍涵蓋那些與個資有關之流程或應用系統。					
	5	個資管理現況評估	本項為選擇性活動，組織可透過個資管理整體準備度評估問卷，對個資管理的現況進行評估，以瞭解目前在個資管理相關領域準備度較為不足之處，並針對主要差異項目進行提升與改善，亦可將準備度評估結果，做為未來提升比較之參考基準。					
	6	個資項目盤點	盤點組織所擁有之個資項目內容，包括個資項目之類別、目的、來源、欄位、數量、型態、相關的生命週期活動及相關利害關係人等，以利後續進行個資之衝擊分析、衝擊評鑑、保護及管理等活動。					
	7	個資衝擊分析	藉由適當的衝擊評估與分析活動，瞭解個資項目或針對處理大量個資之應用系統，所可能面臨之個資洩露的弱點與威脅，及可能造成組織的衝擊與損失，以便及早採取可行之防範對策或					

階段	編號	檢核項目	說明	是	部分	否	不適用	備註
			行動方案，避免個資洩露事故之發生。					
	8	個資風險評估	針對組織所擁有個資項目，依據其個資類別(如一般個資或特種個資)與數量、個資之機密性／完整性／可用性被破壞時會對組織／資產／人員造成的傷害等構面，進行個資風險評估作業，以瞭解個資項目的衝擊等級，並彙整相關個資衝擊分析結果，做為後續規劃安全控制措施之參考依據。					
	9	安全控制措施規劃	組織於進行個資風險評估後，依法規命令與組織可運用之資源，並參考個資保護技術安全控制項目基準值建議表，規劃組織內不同衝擊等級之個資保護技術方案與管理程序。					
執行階段	1	確立人員權責角色	依據組織內個資項目的生命週期，建立組織人員對應各階段活動的個資存取權責與角色，以確保組織對個資的蒐集、處理及利用等活動，符合相關法規命令與組織的個資管理政策，同時做為個資管理程序與安全控制措施的運作基礎。					
	2	建立個資管理程序	依據個資相關法規命令、組織個資管理政策，建立組織之個資管理流程與程序，降低個資洩露或違反相關法規命令的風險。					

階段	編號	檢核項目	說明	是	部分	否	不適用	備註
	3	建立安全控制措施	依據個資相關法規命令、組織個資管理政策及個資安全控制措施規劃，建立組織相關個資管理安全控制措施，降低個資洩露或違反相關法規命令的風險。					
	4	個資委外作業管理	針對個資委外作業，依據個資相關法規命令、組織個資管理政策及個資安全控制措施規劃，透過相關委外契約要求及稽核活動，確保委外作業建立必要的個資管理流程、程序及安全控制措施。					
	5	宣導與教育訓練	依據組織個資管理之目標與需求，建立並實施個資管理相關人員訓練計畫。					
檢查階段	1	個資管理報告檢視	運用 PDCA 機制，依據個資管理政策與目標，定期與不定期檢視個資管理活動與紀錄，或進行趨勢分析。針對可能無法達到或未達到目標之項目，適時提出行動方案以持續提升組織個資管理成效。					

階段	編號	檢核項目	說明	是	部分	否	不適用	備註
	2	個資管理稽核活動	運用 PDCA 機制，規劃定期與不定期對組織個資管理，包括個資委外作業活動的稽核，以發掘未落實執行之活動或潛在改善之機會。針對稽核發現提出矯正預防行動方案，以持續提升組織個資管理成效。					
	3	個資事故追蹤處理	因應個資事故通報與處理回應，包括對於個資事故可能需要之數位證據與數位鑑識處理上的需求等，建立相關作業程序與人員職責角色分派，並與組織相關之資安事故程序予以整合運作，以發揮流程運作之效率。					
行動階段	1	管理組織審查會議	針對設定期間個資管理相關重要議題與績效，進行階段性審查，並與相關利害關係人溝通個資管理的成效。對重大計畫或議題進行決策，並提供後續個資管理活動所需之相關資源。					
	2	個資管理改善計畫	運用 PDCA 機制，分析並彙整相關可提升個資管理活動的潛在機會點，提出個資管理改善計畫，追蹤檢視執行成果，持續改善提升組織的個資管理系統。					

資料來源： 本計畫整理

附件2　個人資料保護管理要點範例

法務部個人資料保護管理要點(已核定，尚未下達生效)

規定	說明
壹、總則	第一章章名
一、法務部（以下簡稱本部）為落實個人資料之保護及管理，特設置本部個人資料保護管理執行小組（以下簡稱本小組），並訂定本要點。	明定訂定本要點及設置法務部個人資料保護管理執行小組之目的。
二、本小組之任務如下： (一)本部個人資料保護政策之擬議。 (二)本部個人資料管理制度之推展。 (三)本部個人資料隱私風險之評估及管理。 (四)本部各單位（以下簡稱各單位）專人與職員工之個人資料保護意識提升及教育訓練計畫之擬議。 (五)本部個人資料管理制度基礎設施之評估。 (六)本部個人資料管理制度適法性與合宜性之檢視、審議及評估。 (七)其他本部個人資料保護、管理之規劃及執行事項。	明定執行小組之任務。
三、本小組置召集人及執行秘書各一人，由部長指定之；委員十一人由各單位指派專人（科長以上）一人擔任。本小組幕僚工作由本部法律事務司辦理；為強化幕僚功能，協助辦理幕僚工作，並得邀請本部各單位人員參與幕僚作業。	鑑於公務機關在個人資料保護及管理上事權統一之重要，爰明定本小組召集人、執行秘書及委員之組成，及幕僚工作之負責單位，以利有效推動個人資料保護相關事務。
四、本小組會議視業務推動之需要，不定期召開，由召集人主持；召集人因故不能主持會議時，得指定委員代理之。本小組會議開會時，得邀請有關業務單位、所屬機關人員、相關機關代表或學者專家出（列）席。	明定本小組會議召開之期間、主持人及得邀請出列席之人員。

規定	說明
五、各單位應指定專人辦理下列事項： (一)辦理當事人依個人資料保護法（以下簡稱本法）第十條及第十一條第一項至第四項所定請求事項之考核。 (二)辦理本法第十一條第五項及第十二條所定通知事項之考核。 (三)本法第十七條所定公開或供公眾查閱。 (四)本法第十八條所定個人資料檔案安全維護。 (五)依第二點第四款所為擬議之執行。 (六)個人資料保護法令之諮詢。 (七)個人資料保護事項之協調聯繫。 (八)單位內個人資料損害預防及危機處理應變之通報。 (九)本部個人資料保護政策之執行、單位內個人資料保護之自行查核。 (十)其他單位內個人資料保護管理之規劃及執行。	為落實個人資料保護法第十七條及第十八條公務機關應公開事項及應指定專人 辦理個人資料檔案安全維護等規定，並妥適處理當事人依據本法第十條、第十一條及第十二條所定權利向本部提出之請求，爰規定本部應指定專人，辦理或考核前述相關事項之執行，以確實執行本法相關規定。
六、本部應設置個人資料保護聯絡窗口，辦理下列事項： (一)公務機關間個人資料保護業務之協調聯繫及緊急應變通報。 (二)以非自動化方式檢索、整理之個人資料安全事件之通報。 (三)重大個人資料外洩事件之民眾聯繫單一窗口。 (四)本部個人資料專人名冊之製作及更新。 (五)本部個人資料專人與職員工教育訓練名單及紀錄之彙整。	明定本部應設置個人資料保護聯絡窗口及其辦理事項。
貳、個人資料範圍	第二章章名
七、本部保有本法第六條有關醫療與犯罪前科之個人資料檔案名稱如下： (一)矯正機關通報傳染病收容人異動名單。	明定本部保有特種資料之個人資料檔案名稱，相關個人資料檔案之類別包括通報傳染病收容人醫療與犯罪前科、保外醫治醫療與犯罪前科、收

規定	說明
(二)獄政系統保外醫治月報表。 (三)矯正資料庫。 (四)刑案資訊整合系統資料庫。 (五)毒品成癮者單一窗口服務系統資料庫。 (六)檢察書類檢索系統資料庫。	容人醫療與犯罪前科、刑案資訊及檢察書類檢索犯罪前科、毒品成癮者醫療與犯罪前科等。
八、本部蒐集、處理或利用個人資料之特定目的，以本部依適當方式公開者為限。有變更者，亦同。	明定本部保有個人資料特定目的之項目，將依本法第十七條規定，以適當方式供公眾查閱，並以本部依適當方式公開者為限。其有變更者，亦同。目前本部保有個人資料之特定目的如下：人事行政管理、公共衛生、公職人員財產申報業務、立法或立法諮詢、犯罪預防、刑事偵查、執行、矯正、保護處分或更生保護事務、刑案資料管理、兵役行政、社會服務或社會工作、法律服務、退撫基金或退休金管理、教育或訓練行政、採購與供應管理、會計與相關服務、資訊與資料庫管理、發照與登記、其他中央政府、其他公共部門、其他司法行政業務、其他地方政府事務、其他諮詢與顧問服務、統計與相關服務、犯罪被害人保護、其他為執行法定職務而經本部新增公告之特定目的。
叁、個人資料之蒐集、處理及利用	第三章章名
九、各單位對於個人資料之蒐集、處理或利用，應確實依本法第五條規定為之。遇有疑義者，應提請本小組研議。	本法第五條規定個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。各單位於執行上有疑義者，應由專人報請本小組研議。

規定	說明
十、各單位蒐集當事人個人資料時，應明確告知當事人下列事項。但符合本法第八條第二項規定情形之一者，不在此限： (一)機關或單位名稱。 (二)蒐集之目的。 (三)個人資料之類別。 (四)個人資料利用之期間、地區、對象及方式。 (五)當事人依本法第三條規定得行使之權利及方式。 (六)當事人得自由選擇提供個人資料時，不提供對其權益之影響。	為使當事人知悉其個人資料為本部所蒐集、本部進行蒐集之目的、資料類別、利用相關事項及當事人所得行使之權利等，爰明定除符合本法第八條第二項規定情形外，各單位於向當事人蒐集個人資料時，應明確告知本法第八條第一項所定六款事項。
十一、各單位蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一款至第五款所列事項。但符合本法第九條第二項規定情形之一者，不在此限。 前項之告知，得於首次對當事人為利用時併同為之。 第一項非由當事人提供之個人資料，於本法修正施行前即已蒐集者，除有本法第九條第二項所定免為告知之情形外，應自本法修正施行之日起一年內完成本法第九條第一項所列事項之告知。	一、本法第八條要求直接蒐集個人資料時，應進行告知，另 針對個人資料之間接蒐集態樣，本法第九條第一項亦要求於處理或利用前，告知當事人資料來源及其相關事項，俾使當事人明瞭其個人資料被蒐集情形，爰於第一項明定蒐集非由當事人提供之個人資料時，應於處理或利用前，向當事人告知個人資料來源及本點第十條第一項(同本法第八條第一項)第一款至第五款所列事項。 二、另依本法第九條第三項規定，針對間接蒐集個人資料之告知，得於首次對當事人為利用時併同為之，爰明定第二項，期能確實執行。 三、又本法第五十四條規定，本法修正施行前非由當事人提供之個人資料，應自本法修正施行之日起一年內完成告知，逾期未告知而處理或利用者，以違反第九條規定論處，爰於第三項明定本部就本法修正前已蒐集、非由當事人提供之個人資料，應自本法修正施行之日起一年內完成

規定	說明
	本法第九條第一項所列事項之告知。
十二、各單位依本法第十五條第二款及第十六條但書第七款規定經當事人書面同意者，應取得當事人同意書。	為符合法第十五條及第十六條對於個人資料蒐集、處理及利用之要件，爰明定應取得當事人同意書。
十三、各單位依本法第十五條或第十六條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。 各單位依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。對於個人資料之利用，不得為資料庫之恣意連結，且不得濫用。	一、各單位依本法第十五條或第十六條規定對個人資料為蒐集、處理、利用時，應詳為審核其是否符合法定要件，爰為第一項規定。 二、各單位依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄，俾以管理查核，爰明定第二項。 三、總統政見執行追蹤事項之人權政策（編號286）關於「政府資料庫不得恣意聯結、濫用個人資料、侵害人民隱私」之執行，爰為第三項規定。
十四、本部保有之個人資料有誤或缺漏時，應由資料蒐集單位簽奉核定後，移由資料保有單位更正或補充之，並留存相關紀錄。 因可歸責於本部之事由，未為更正或補充之個人資料，應於更正或補充後，由資料蒐集單位以通知書通知曾提供利用之對象。	一、為維護個人資料之正確，除當事人得請求 本部更正或補充外，依本法第十一條規定，公務機關亦負有更正或補充之義務，爰於第一項之規定。 二、為符合本法第十一條第五項規定，於第三項明定於更正或補充後，應通知曾提供利用之對象。
十五、本部保有之個人資料正確性有爭議者，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料。但符合本法第十一條第二項但書情形者，不在此限。 個人資料已停止處理或利用者，資料保有單位應確實記錄。	為符合本法第十一條第二項所定公務機關停止處理或利用正確性有爭議之個人資料之規定，爰明定其處理程序。
十六、本部保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除、停止處理或利用。但符合本法第十一條第三項但書情形者，不在此限。	為符合本法第十一條第三項所定公務機關對於個人資料蒐集之特定目的消失或期限屆滿時，除因執行職務所必須或經當事人書面同意者外，應刪除、停止處理或利用該個人資料之

規定	說明
個人資料已刪除、停止處理或利用者，各該單位應確實記錄。	規定，爰明定其處理程序。
十七、各單位依本法第十一條第四項規定刪除、停止蒐集、處理或利用個人資料者，應簽奉核定後移由資料保有單位為之。 個人資料已刪除、停止蒐集、處理或利用者，資料保有單位應確實記錄。	為符合本法第十一條第四項所定公務機關如違反本法規定蒐集、處理或利用個人資料者，應刪除、停止蒐集、處理或利用該個人資料之規定，爰明定其處理程序。
十八、本部遇有本法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，經查明後，應由資料外洩單位以適當方式儘速通知當事人。	為使當事人迅速知曉個人資料遭到竊取、洩漏、竄改或遭其他方式侵害，爰依本法第十二條規定，明定本部應於違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害時，應儘速查明後由資料外洩單位以適當方式通知當事人。
肆、當事人行使權利之處理	第四章章名
十九、當事人依本法第十條或第十一條第一項至第四項規定向本部為請求時，應檢附相關證明文件。 前項書件內容，如有遺漏或欠缺，應通知限期補正。 申請案件有下列情形之一者，應以書面駁回其申請： (一)申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正。 (二)有本法第十條但書各款情形之一。 (三)有本法第十一條第二項但書或第三項但書所定情形之一。 (四)與法令規定不符。	一、依據本法第十條及第十一條第一項至第四項規定，當事人就公務機關蒐集之個人資料，得向公務機關請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除。為期明確申請程序，爰於第一項規定當事人向本部行使本法上開規定權利時，應填具申請書，並檢附應備文件為之。 二、當事人之申請書件內容如有遺漏或欠缺時，應先通知限期補正，不宜逕予駁回，爰明定第二項規定。 三、針對當事人所得行使之權利，本法第十條及第十一條第二項、第三項亦分別定有相關除外規定，爰於第三項規定凡有本法第十條但書各款情形之一或有本法第十一條第二項但書或第三項但書情形者，本部應以書面駁回其申請。此外，當事人申請書件內容有遺漏或欠缺，經通知補正逾

規定	說明
	期未補正，或有其他與法令規定不符之情形者，亦應駁回當事人之申請。
二十、當事人依本法第十條規定提出之請求，應於十五日內為准駁之決定。 前項准駁決定期間，必要時得予延長，延長期間不得逾十五日，並應將其原因以書面通知請求人。	為明確當事人依本法第十條規定，針對本部蒐集之個人資料所提出之請求查詢、提供閱覽或製給複製本之處理時程，爰依本法第十三條第一項前段規定，於第一項規定凡受理當事人依本法第十條規定提出之請求時，由各承辦單位簽報單位主管，並於十五日內為准駁之決定。另依本法第十三條第一項後段規定，於第二項明定得予延長准駁期間及應將原因通知請求人之規定。
二十一、當事人請求查詢、閱覽或製給個人資料複製本者，適用「法務部及所屬機關提供政府資訊收費標準」收取費用。 當事人閱覽其個人資料，應由承辦單位派員陪同為之，並依「法務部受理申請提供政府資訊及閱覽卷宗須知」辦理。	一、對於當事人查詢或閱覽個人資料或製給個人資料複製本之請求，依本法第十四條規定得酌收必要成本費用，爰予明定。 二、為確保本部保有個人資料之安全與完整性，爰於第三項規定當事人應由承辦單位派員陪同，始得閱覽其個人資料，並依「法務部受理申請提供政府資訊及閱覽卷宗須知」辦理。
二十二、當事人依本法第十一條第一項至第四項規定提出之請求，應於三十日內為准駁之決定。 前項准駁決定期間，必要時得予延長，延長期間不得逾三十日，並應將其原因以書面通知請求人。	一、為明確當事人依本法第十一條第一項至第四項規定，向本部提出之請求更正、補充、停止處理、停止利用或刪除個人資料之處理時程，爰依本法第十三條第二項前段規定，於第一項明定受理當事人依本法第十一條第一項至第四項規定提出之請求時，應於三十日內為准駁之決定。 二、另依本法第十三條第二項後段規定，於第二項明定得予延長准駁期間及應將原因通知請求人之規定。
二十三、本部保有之個人資料檔案之公開，仍適用政府資訊公開法或其他法律規定。	考量本部保有之個人資料檔案，可能屬於政府資訊公開法第十八條第一項第一款至第九款或依其他法律規

規定	說明
	定應限制公開或不予提供之資訊，爰明定個人資料檔案之公開，仍適用政府資訊公開法或相關法律規定。
伍、個人資料檔案安全維護	第五章章名
二十四、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本部指定之個人資料檔案安全維護專人，應依本要點及相關法令規定辦理個人資料檔案安全維護事項。	為符合本法第十八條規定之要求，爰明定本部指定之個人資料檔案安全維護專人，應依本要點及相關法令規定，辦理個人資料檔案安全維護事項。
二十五、個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。	為強化個人資料檔案之管理，本部應針對保有之個人資料檔案，建立分級管理制度，並應參考「法務部及所屬機關人員資訊安全管理規範」(民國九十六年三月十三日發布，九十九年二月四日修正)等相關規定，針對可能接觸個人資料檔案之人員，建立人員安全管理規範。
二十六、為強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立個人資料檔案安全稽核制度，由資安稽核小組定期查考。 前項個人資料檔案資訊系統之帳號、密碼、權限管理及存取紀錄等相關管理事宜，依「法務部及所屬機關資訊系統存取控制管理規範」辦理之。 第一項個人資料檔案安全稽核之運作組織、稽核頻率及稽核所應注意之相關事項，依「法務部及所屬機關資訊安全稽核作業管理規範」辦理之。	一、本部現行依「法務部及所屬機關資訊安全稽核作業管理規範」由資安稽核小組來辦理資安稽核有關之業務，且因本部政風司負責公務機密檢查業務(含個資洩密事件)，本部資安稽核小組之成員亦由政風司主導使用稽核業務，而本部法律事務司係主責個人資料保護有關之業務，資訊處建議本部日後辦理資訊安全內、外部稽核作業時，將邀請法律事務司指派人員擔任查核小組成員，屆時與政風司共同查核有關個人資料保護有關之事項。 二、為避免儲有個人資料檔案之資訊系統，遭非法授權存取，本部應強化個人資料檔案資訊系統之存取安全，以妥適維護資料機密性。並為明確、落實資訊系統之安全維護，明定應依「法務部及所屬機關資訊系統存

規定	說明
	取控制管理規範」(民國九十九年一月二十六日發布)為之。 三、為確保個人資料資料安全無虞，本部應建立個人資料檔案安全稽核制度。為明確稽核制度之程序與運作，本部應依「法務部及所屬機關資訊安全稽核作業管理規範」(九十六年三月十三日發布)，辦理相關稽核作業事項。
二十七、各單位遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，如屬以非自動化方式檢索、整理之個人資料外洩事件，應進行緊急因應措施，並迅速通報至本小組;如屬以自動化機器檢索、整理之個人資料外洩事件，應依「法務部及所屬機關資通安全事件緊急應變計畫」迅速通報至本部資通安全處理小組之資安聯絡人員上網通報至行政院國家資通安全會報緊急應變中心。	鑑於行政院國家資通安全會報針對重大資安事件之處置，訂有「國家資通安全通報應變作業綱要」，本部亦依該綱要，訂有「法務部及所屬機關資通安全事件緊急應變計畫」，爰明定個人資料檔案，發生遭人為惡意破壞毀損、作業不慎等重大內部危安事件，或發生駭客攻擊等非法外力入侵事件，如屬以非自動化方式檢索、整理之個人資料外洩事件，應進行緊急因應措施，並迅速通報至本小組；如屬以自動化機器檢索、整理之個人資料外洩事件，依該前述應變計畫，應進行緊急應變處置並迅速通報至本部資通安全處理小組之資安聯絡人員(由本部資訊處指派專人擔任) 上網通報至行政院國家資通安全會報緊急應變中心。
二十八、個人資料檔案安全維護工作，除本要點外，並應符合行政院及本部訂定之相關資訊作業安全與機密維護規範。	針對個人資料檔案之安全維護，行政院已訂有「行政院及所屬各機關資訊安全管理規範」與「行政院及所屬各機關資訊安全管理要點」，本部亦訂有相關規定，爰規定本部就個人資料檔案之安全維護，除本要點外，尚應符合相關規範。
陸、附則	第六章章名

規定	說明
二十九、本部依本法第四條規定委託蒐集、處理或利用個人資料者，適用本要點。	依本法第四條規定，受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關，爰明定受本部委託蒐集、處理或利用個人資料者，適用本要點規定。

資料來源： 法務部全球資訊網

附件3　個人資料保護與隱私政策範例

1 目的

為規範個人資料之蒐集、處理及利用、促進個人資料之合理利用、展現組織對個人資料與隱私保護之決心，特此訂定個人資料與隱私保護管理最高指導方針，以建立安全、可信賴之資訊服務，並確保組織執行業務工作皆符合相關法規之要求，維持業務持續運作，降低個人資料遭受不當揭露之風險，進而保障相關人員之權益，確保組織個人資料保護與資訊安全，維護組織聲譽與提供永續服務。

2 目標

2.1 組織在執行外部業務與內部行政作業時，有關個人資料之蒐集、處理及利用等活動，應符合機密性、完整性及可用性，使危及資料保護相關事故發生機率降至最低。

2.2 建立組織與個人資料保護相關之標準作業程序，避免人為作業疏失及意外，加強同仁個人資料保護安全意識。

2.3 保護組織所管理之個人資料，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為。

3 原則

3.1 執行各項業務專案與內部行政作業因需要所蒐集之個人資料，除非法律規定或經當事人同意分享個人資料，所有資料不應逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

3.2 應考量相關法律規章及營運要求，進行個人資料之風險評估，採取適當安全措施，以確保組織善盡個人資料良善保護之責。

3.3 個人資料存取權限之賦予，應考量業務需求之最小權限、實施權責區

隔與獨立性審查。

3.4 所蒐集之個人資料其正確性受到適當的維護，且確保為最新資料。

3.5 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行法定職務或業務所必須或經當事人書面同意者，不在此限。

3.6 依據個人資料保護法之規定，應審慎處理與保護個人資料。

3.7 違反本政策與個人資料保護法等相關規範，應依相關法規和組織人事規定辦理。

4 適用範圍

本政策適用範圍為組織所有相關同仁、約聘人員、委外人員、供應者等執行業務專案與內部行政作業所涉及的個人資料之蒐集、處理及利用等活動；參考依據為個人資料保護法。

附件4　個資管理整體準備度評估問卷

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
告知/目的	是否已指派組織內負責個人資料規劃的人員？			
告知/目的	是否已有文件載明負責個人資料規劃人員的責任、授權層級、以及報告機制？			
告知/目的	是否已明確規範對相關負責個資管理人員的績效要求與衡量方式，並進行績效符合性的審查？			
告知/目的	是否已有經管理階層核准，宣告當事人個人資料如何與何時被蒐集、利用、以及保護之個人資料管理政策？			
告知/目的	個人資料管理政策是否定期進行審查及更新？			
告知/目的	個人資料管理政策是否已合併在組織的道德規範內，並發布至組織全體？			
告知/目的	個人資料管理政策是否適用於內部員工資料？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關蒐集個人資料的理由？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關那些個人資料為必要？那些為非必要可選擇不提供？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關個人資料之利用與處理方式？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關在何種情況下個人資料將會被交換至那些不同的對象？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人/員，有關個人資料的安全維護方式？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關當事人如何存取其個人資料？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織人員，有關當事人如何更正其個人資料？			
告知/目的	組織是否提供清楚與明顯的說明予當事人或組織			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
	人員，有關組織內負責人員的姓名與聯絡資訊			
告知/目的	組織若進行蒐集法定須由監護人代理之年齡的兒童及少年之個人資料，是否有明確說明非必要的兒童及少年個人資料蒐集是被禁止的，同時當事人的監護人有權要求審閱或提出刪除其當事人的個人資料，並有權要求停止蒐集或拒絕使用其當事人之個人資料			
告知/目的	組織是否明確規範不對特種個資(醫療、基因、性生活、健康檢查、犯罪前科)進行蒐集、利用及處理？			
告知/目的	進行個人資料蒐集時是否遵循所屬行業別的法規或公約(例如 金融、保險、社會安全、健康照護等)？			
告知/目的	進行個人資料蒐集時是否遵循所屬縣市地方政府規定？			
告知/目的	進行個人資料蒐集時是否遵循國家之個人資料保護法、相關施行細則及中央政府行政命令？			
告知/目的	進行個人資料蒐集時是否遵循國際法規、條約及國際組織規範標準？			
告知/目的	若組織進行個人資料蒐集、利用及處理時，擁有不止一個管轄權，每個管轄權對可識別個人資料之監管與控制方式是否已文件化？			
告知/目的	若組織進行個人資料蒐集、利用及處理時，擁有不止一個管轄權，對於每個管轄權的隱私要求是否已文件化？			
告知/目的	若組織進行個人資料蒐集、利用及處理時，對不受法律規範的管轄權是否簽有約定或合約，以符合相關隱私需求？			
告知/目的	是否已明確規範對相關管轄權的績效要求與衡量方式，並進行績效符合性的審查？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
告知/目的	對相關管轄權與方案是否會產生任何法定衝突，是否已尋求法律意見或制定政策？			
告知/目的	是否已揭示組織內含有個人資料的資料庫與使用目的，符合資料保護相關主管機關的要求？			
告知/目的	組織是否告知員工，其個人薪資資料在內部將會如何利用。以及若有需要，資料將如何與其他組織間進行交換？			
告知/目的	組織是否告知員工，其個人員工福利資料在內部將會如何利用。以及若有需要，資料將如何與其他組織間進行交換？			
告知/目的	組織是否告知員工，其於組織或商業夥伴中的個人優惠在內部將會如何利用。以及若有需要，資料將如何與其他組織間進行交換？			
告知/目的	組織是否告知有關組織是否監控員工的工作場所活動和通訊？			
告知/目的	組織是否告知有關對組織員工和當事人的獨立政策？			
告知/目的	組織是否告知當事人是否有可預防通訊被監控的機制？			
告知/目的	組織是否有採用相關網路隱私標章計劃(例如 TRUSTe，WebTrust 2.0 以上…等)？			
告知/目的	組織是否已提供當事人，有關電話監控的資訊？			
告知/目的	組織是否已提供當事人，有關傳真監控的資訊？			
告知/目的	組織是否已提供當事人，有關錄像監視監控的資訊？			
告知/目的	組織是否已提供當事人，有關應用 / 作業系統紀錄監控的資訊？			
告知/目的	組織是否已提供當事人，有關瀏覽器 Cookie 檔案監控的資訊？			
告知/目的	組織是否已提供當事人，有關電子郵件監控的資訊？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
告知/目的	組織是否已提供當事人，有關網際網路 / Web 瀏覽監控的資訊？			
自主/同意	從當事人蒐集的資料是否採事先知會、自願與公平的方式進行，而非透過欺騙的技巧？			
自主/同意	被蒐集個人資料之當事人是否能判斷其個人資料將會與第三方分享？			
自主/同意	被蒐集個人資料之當事人是否能選擇那些對象將可獲得當事人之個人資料？			
自主/同意	被蒐集個人資料之當事人是否能將已被蒐集的個人資料從組織的資料庫中解除？			
自主/同意	被蒐集個人資料之當事人是否可明確識別出蒐集當事人個人資料之組織？			
自主/同意	被蒐集個人資料之當事人是否能判斷蒐集其個人資料的網站是由誰在負責營運(例如：是否為委外管理)？			
自主/同意	透過第三方蒐集個人資料是否由被蒐集個人資料之當事人同意？並提供當事人受委託第三方與委託方之間證明委任關係的文件？			
自主/同意	由第三方蒐集的個人資料，使用於二次使用用途(例如：服務強化、資源管理或研究目的)是否經被蒐集個人資料之當事人或員工之同意？			
自主/同意	是否有進一步的程序 ，用於延續取得當事人同意當逾越原先告知特定目的以外的個人資料處理或利用的需求？			
自主/同意	當有跨不同管轄的規劃需要當事人同意蒐集、利用及或揭露個人資料，是否事先協調各個不同管轄內容後 ，提供予當事人選擇是否同意？			
自主/同意	是否有方法讓當事人可指定其資料將如何被組織利用？			
自主/同意	是否有方法讓當事人可指定其資料未來將如何被利用？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
自主/同意	是否有方法讓當事人選擇當其資料被利用前是否需被知會？			
自主/同意	是否有方法讓當事人可指定其資料是否會被分享至第三方？			
自主/同意	是否有方法讓當事人當不同型式資料要被進行二次利用或分享至第三方時，可選擇”退出”？			
自主/同意	是否可讓當事人透過線上或其他管道方式提出對個人資料蒐集、利用或處理的異議或意見？			
自主/同意	對於敏感性個人資料的蒐集或利用，是否事先取得當事人明確的同意(明確的”選定”)？			
自主/同意	在進行市場行銷活動前，是否比對組織的資料庫內容和組織內或所從事產業別的”禁止使用名單”和”退出名單”？			
自主/同意	當當事人資料被利用在不屬原本目標與指定的其他利用時，是否提供當事人”退出”的選擇？			
自主/同意	針對未滿法定須由監護人代理之年齡的兒童及少年之個人資料的蒐集、利用及處理，組織是否提供可供當事人監護人回傳同意的機制？			
自主/同意	當當事人收到組織內外部額外的市場行銷資訊時，是否提供當事人”退出”接收此類資訊的選擇？			
資料蒐集與保存	組織是否僅蒐集與目的範圍有關的個人資料，除當事人同意與法律規定外，不蒐集過度的個人資料？			
資料蒐集與保存	組織是否沒有透過商業合作夥件或聯盟蒐集或提供各別的個人資料？			
資料蒐集與保存	負責與當事人互動的員工是否已進行個人資料蒐集準則的訓練，以及瞭解那些類型的資料是相關的，那些是過多的資料？			
資料蒐集與保存	是否有對兒童及少年識別其年齡是否適用於個人資料保護法與兒童及少年保護法的範圍			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
資料蒐集與保存	填寫個人資料的紙本或線上表單，是否包括清楚說明個人資料被蒐集利用的特定目的？			
資料蒐集與保存	填寫個人資料的紙本或線上表單內容，是否有包含對當事人權利的解釋？			
資料蒐集與保存	填寫個人資料的紙本或線上表單內容，是否標示必要與選擇性的資料欄位(以及輸入選擇性資料欄位的益處)？			
資料蒐集與保存	填寫個人資料的紙本或線上表單內容，是否包含”退出”選項與及對當事人權益之影響？			
資料蒐集與保存	個人資料是否僅保存於個人資料宣告目的所需的期間？			
資料蒐集與保存	存有歐洲地區當事人個人資料之資料庫，是否已向該國個人資料保護主管機關註冊？			
資料蒐集與保存	資料蒐集是否僅限於適當的營運目的，所有蒐集到的個人資料是否都是為了所宣告的營運目的所需？			
資料蒐集與保存	是否能利用較少的資訊或是總概性的資訊即可達成營運目的？			
資料蒐集與保存	對於並無立即利用需求，但為營運目的須蒐集與保存的資料類型，是否僅在合法的範圍內蒐集與保存？			
資料蒐集與保存	是否依據法律規定、組織政策及合約/協議等，發出說明資料蒐集原因的通知？			
資料蒐集與保存	是否有可供提出通知放棄蒐集個人資料之流程？			
資料蒐集與保存	是否有流程來確認與記錄當組織進行資料蒐集時，已進行相關告知事宜？			
資料蒐集與保存	組織使用個人資料以履行協議或交易前，是否已告知所蒐集資料之當事人？			
資料蒐集與保存	是否已建立個人資料和跨管轄蒐集、利用或揭露間的明確關係？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
資料蒐集與保存	是否有文件化記錄每個管轄所蒐集個人資料的目的與彼此間的協調方式？			
資料蒐集與保存	是否有考量將資料蒐集傳遞路徑最小化的所有選項？			
資料蒐集與保存	當需要進行跨多重資料庫連結時，是否使用如單一登入(SSN)機制的個人識別？			
資料蒐集與保存	是否已建立分析與協調各管轄間，對個人資料紀錄保存時間長度的指引文件與程序？			
資料蒐集與保存	有關個人資料保存的指引文件與程序，是否包含對個人資料保存時間的最短與最長期間？			
資料蒐集與保存	是否有流程來文件化如何進行各年代個人資料的追蹤與報告？			
資料蒐集與保存	是否有文件化的指引與程序，來管理個人資料之銷毀、刪除或合併轉換？			
資料蒐集與保存	當個人資料被銷毀時是否留有處理記錄？此處理紀錄中是否亦不含個人資料？			
資料蒐集與保存	是否已建立分析與協調各管轄間，當進行個人資料紀錄銷毀時的需求？			
資料蒐集與保存	是否有制定程序來治理跨轄區進行個人資料的銷毀？			
資料蒐集與保存	若個人資料被用於新的目的時，組織是否有完成此新目的的授權與文件紀錄？			
利用與揭露	個人資料之處理與利用係依據組織之隱私權政策，並於資料蒐集時告知當事人相關訊息？			
利用與揭露	敏感性個人資料用於統計時，是否採用匿名方式進行？			
利用與揭露	組織是否已評估跨境儲存或交換之個人資料檔案，是否符合各區域之法令法規要求與違反之影響(包含電子，書面及備份資料)？			
利用與揭露	若組織採用資料倉儲、資料採礦及各種自動化資料處理機制，是否已評估相關技術功能或機制處理程			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
	序符合擊隱私權相關規定？			
利用與揭露	是否有足夠的控管機制於揭露個人資料時不致違反組織之隱私權政策與管理架構？			
利用與揭露	組織員工是否有教育訓練如何辨識個人資料的要求，且不揭露個人資料予假冒當事人身分的要求？			
利用與揭露	特定揭露資訊的需要，是否有經由管理階層的正式核准？			
利用與揭露	所有特定之資料揭露情形是否有留存紀錄？			
利用與揭露	在個人資料傳遞至第三方之前，是否有審視移除相關當事人已選擇”退出”的資料內容？			
利用與揭露	組織之隱私權政策與管理規範，是否隨資料傳遞至第三方(例如：組織之附屬機構，代理商，委外服務業者，直銷業者，在其他國家的私人企業)而跟隨移轉？			
利用與揭露	與第三方的合約內容，是否包含相關隱私和安全條款？			
利用與揭露	是否維護個人資料之使用紀錄？			
利用與揭露	資料庫中特定資料傳遞予其他對象時，是否保存有系統事件紀錄？			
利用與揭露	委外服務或外部顧問是否接簽署保密切結書？			
利用與揭露	組織是否有垃圾郵件防治政策與作業程序？			
利用與揭露	針對法定須由監護人代理之年齡的兒童及少年的個人資料，當其監護人只同意內部使用時，組織是否有控管機制防止資料揭露或轉移至第三方？			
正確性	組織現有的資料管理程序及資料庫控管，是否可確保資料的完整性？			
正確性	組織是否與當事人進行定期聯繫，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否提供容易使用的資料更新方式，以確保所蒐集之個人資料為最新資料？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
正確性	組織是否提供當事人皆可自由提出並進行資料更新的方式，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否進行內部資料庫比對，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否與外部資料庫進行比對，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否定期審查個人資料輸入及資料庫更新情形，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否有文件化的作業程序定義何種個人資料查閱或公開的方式，以確保所蒐集之個人資料為最新資料？			
正確性	組織是否有文件化的程序定義組織對個人資料的蒐集，利用及揭露之存取資料？			
正確性	系統是否被設計為可協助當事人於存取其個人資料時，對作業中斷的影響降至最小？			
正確性	組織是否將資料更正通知相關第三方單位？以確保所蒐集之個人資料為最新資料？			
正確性	組織是否已分析並協調不同管轄間處理個人資料存取時，已實施充足的管理程序，以確保符合個人資料保護法所涵蓋或未涵蓋的範圍？			
正確性	組織對內部蒐集或自外部取得的資料，是否有程序化的評估控制來確認其品質？			
正確性	當進行應用系統及資料庫之開發時，是否有考量相關隱私政策的程序？			
正確性	當選擇套裝應用系統時，是否有考量相關隱私政策的程序？			
正確性	當進行營運流程設計時，是否有考量相關隱私政策的程序？			
正確性	當採購電話 / 錄音 / 錄影設備時，是否有考量相關隱私政策的程序？			
正確性	組織是否有建立程序來辨識那些個人資料有被要			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
	求更正或刪除？			
正確性	組織是否提供當事人易於提出要求將其個人資料之狀態予以註記的方式？			
正確性	組織是否有相關程序以處理當事人對個人可辨識資料之管理提出異議或資料修正的要求？			
正確性	組織內負責個人資料的管理人員，是否知道當事人的存取權限，以及當事人正式或非正式的建議，抱怨及申訴的跨管轄程序需求？			
正確性	是否有建立紀錄及定期審查客訴與處理程序，以建立資訊管理實作與標準的改善方案？			
正確性	是否紀錄所有個人資料關鍵屬性之變更？			
正確性	組織是否已建置控制以確保資料庫在進行合併時可維持資料之完整性？			
保護/安全性	是否有資訊安全政策文件？			
保護/安全性	是否有資訊安全組織之指派與安全責任？			
保護/安全性	是否有指定資料檔案之擁有者？			
保護/安全性	是否有將資料依據隱私敏感程度予以分類？			
保護/安全性	是否有足夠強度的認證 / 驗證機制(如帳號密碼驗證、生物辨識)？			
保護/安全性	是否有實體與環境安全管理？			
保護/安全性	是否有主機與網路管理及存取控制管理？			
保護/安全性	是否有人員安全管理？			
保護/安全性	是否有資訊資產的分類及控管措施？			
保護/安全性	是否有資訊安全教育和訓練？			
保護/安全性	是否有入侵偵測設備及資訊安全事故報告？			
保護/安全性	是否有病毒防治機制？			
保護/安全性	是否有營運持續計劃及作業流程？			
保護/安全性	組織是否有充足的存取控制管理邏輯，來限制員工為特定目的存取一般性和敏感性個人資料？			
保護/安全性	是否有適當的儲存媒體存取控制方式以防止員工得以存取敏感性個人資料？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
保護/安全性	是否嚴格限制營運系統之個人資料存取方式？			
保護/安全性	透過網際網路或公眾網路進行個人資料交換時是否採取保護措施(如資料加密)？			
保護/安全性	是否嚴格限制稽核紀錄之存取？			
保護/安全性	是否對聘僱人員之背景資料進行確認以評估其誠信？			
保護/安全性	是否限制合約提供服務者或外部顧問對敏感性資料的存取權限？			
保護/安全性	存有敏感性個人資料之電子儲存媒體及紙本文件(包含磁帶)，是否有足夠安全的銷毀處理方式？			
保護/安全性	針對法定須由監護人代理之年齡的兒童及少年，是否有適當的網站控管措施，以確保符合「個人資料保護法」及「兒童及少年福利法」之要求？例如是否在取得其監護人同意之前即蒐集或利用當事人之個人資料？			
保護/安全性	資料擁有者及管理人員針對配賦的特權帳號之妥適性是否定期審查？			
保護/安全性	是否已有適當的風險管理計畫？			
保護/安全性	是否有特定的風險審查與妥適的安全防護措施，以確保可防止透過任何管道進行未經授權或不適當的存取、蒐集、利用、公開及處理個人資料等行為？			
保護/安全性	是否已有文件化的安全處理程序以執行個人資料之蒐集、傳遞、儲存、處理與存取？			
保護/安全性	是否有適當的控管機制以管理個人資料之新增、修改、刪除之授權？			
保護/安全性	是否只在使用者確切需要且其目的與資料蒐集時一致時才提供資料查詢？			
保護/安全性	是否有與資訊敏感性相對稱的安全性量測方式？			
保護/安全性	是否有適當的營運持續計劃獲應變方式以因應資料外洩或違反隱私權等事故？			
保護/安全性	資料之正確性與安全性是否有適當的維護方式？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
保護/安全性	是否有適當的控管機制以確保資料庫內容之正確性、完整性、安全且僅由被授權的來源所存取？			
保護/安全性	是否採用 SSL 加密方式以提供當事人上傳其資料？			
保護/安全性	是否有文件化的管理程序以詳細規範組織內部如何進行資料存取？			
保護/安全性	是否有文件化的管理程序以詳細規範個別建立或群組授權的特權存取帳號之建立方式？			
保護/安全性	組織是否已針對特定的使用者資料定義利用範圍、安全維護水準及資料隱私為戶方式？			
保護/安全性	是否有適當的軟硬體設定以協助確保存取控制？例如足夠強度的網路防火牆路徑設定限制及網路存取政策？			
保護/安全性	具敏感性資訊是否有加密保護？			
保護/安全性	網站是否採用第三方內容服務供應商之資訊、活動標題或網頁框格？若有採用上述網頁開發技術，網站上是否提供訊息告知即將前往的網頁，已離開安全網站範圍，或進入另一網站服務範圍？			
公開	組織是否已建立個人資料保護政策，且該政策包含對線上與離線作業的政策，如何蒐集、處理、保護個人資料，個人資料利用之期間、地區、對象及方式？			
公開	組織內相關單位(如法務、法令遵循或風險管理、行銷、資訊及工會等)，是否有參與個人資料保護之規劃？			
公開	組織是否已備有個人資料保護聲明，並宣告於官方網站？			
公開	組織是否已備有個人資料保護聲明，並宣告於組織內部網站？			
公開	組織是否已備有個人資料保護聲明，並宣告於組織政策？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
公開	組織是否已備有個人資料保護聲明，並宣告於員工手冊？			
公開	組織是否以淺顯易懂的內容向當事人及商業夥伴聲明個人資料保護政策？			
公開	組織是否將向當事人及商業夥伴聲明個人資料保護政策置於明顯處？			
公開	組織是否在蒐集當事人個人資料前主動提供聲明？			
公開	組織對當事人及商業夥伴聲明之個人資料保護政策內容，是否包含蒐集個人資料之目的？			
公開	組織對當事人及商業夥伴聲明之個人資料保護政策內容，是否包含限制個人資料處理及利用的方式？			
公開	組織對當事人及商業夥伴聲明之個人資料保護政策內容，是否包含組織與個人資料相關之聯繫窗口？			
公開	組織對當事人及商業夥伴聲明之個人資料保護政策內容，是否包含個人資料保護政策適用範圍(譬如那些網頁由組織控管，那些連結網頁由第三方控管)？			
公開	組織是否有當事人個人資料蒐集、利用及處理之目的、政策、常見問題及聯繫方式說明等的訓練計畫？			
公開	組織是否有針對當事人提供或拒絕提供個人資料對其權益之影響說明的訓練計畫？			
公開	組織是否有針對當事人拒絕提供個人資料可能的追索權(若當事人因拒絕提供資料造成的權益受損，應如何追索)的訓練計畫？			
存取	當事人是否可透過網站申請，簡易、清楚、方便地查詢或閱覽其個人資料？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
存取	當事人是否可透過傳真回覆，簡易、清楚、方便地查詢或閱覽其個人資料？			
存取	當事人是否可透過客服中心，簡易、清楚、方便地查詢或閱覽其個人資料？			
存取	當事人是否可透過信件，簡易、清楚、方便地查詢或閱覽其個人資料？			
存取	組織是否提供當事人如何查詢或閱覽其個人資料的方式？			
存取	當事人請求閱覽個人資料時，組織所收取的費用是否合理？			
存取	組織員工是否經由訓練瞭解或透過資訊系統控管那些個人資料可接受當事人請求自行處理，並且免責(譬如醫療、國家機密、法律明文規定等原因)？			
存取	是否管控個人資料存放位置，譬如在那些系統、資料庫或紙本文件等？			
存取	是否管控存放在程式碼及其他加密資料檔中的個人資料？			
存取	組織是否已建立或實施個人資料更正或修改之政策及程序？			
存取	組織是否保存個人資料更正紀錄(書面紀錄或系統紀錄)？			
存取	由受委託第三方負責當事人資料管理時，組織是否訂有當資料有緊急修正需求時通知第三方之程序？			
遵循性與賠償	組織是否提供當事人當進行訴訟或糾紛的處理時，當事人應遵循的方式？			
遵循性與賠償	組織提供進行訴訟或糾紛的處理流程，是否容易瞭解、執行，並且是當事人可負擔的？			
遵循性與賠償	組織是否提供當事人不同的方式可供選擇進行訴訟或糾紛的處理？			
遵循性與賠償	組織管理階層是否持續監督個人資料管理程序之			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
	遵循性？			
遵循性與賠償	組織是否參加產業自律組織以確保遵循個人資料保護法等相關規範？			
遵循性與賠償	組織是否以自我評鑑方式評估個人資料保護之落實與遵行情形？			
遵循性與賠償	組織是否以內部稽核方式評估個人資料保護之落實與遵行情形？			
遵循性與賠償	組織是否以外部稽核方式評估個人資料保護之落實與遵行情形？			
遵循性與賠償	組織是否已識別未落實個人資料保護可能對組織的負面影響(例如：被取消使用認證標章的權利、公眾負面印象、被列入黑名單、被取消產業公會會員資格、刑事調查、強制令、罰款、刑事訴訟等)？			
遵循性與賠償	組織是否對內或外部機構未落實個人資料保護訂有相關的處分方式(例如：解雇員工、取消會員資格、取消使用信任標識或認證標章的權利、制裁等)？			
遵循性與賠償	組織是否向產業工會報告揭露個人資料保護之遵循性？			
遵循性與賠償	組織是否在網站上標示公正認證標章，以揭露個人資料保護之遵循性？			
遵循性與賠償	組織是否公布客訴內容及解決方式，揭露個人資料保護之遵循性？			
遵循性與賠償	是否有協會可提供當事人進行申訴，檢舉組織未落實個人資料保護之情事？			
遵循性與賠償	組織是否規範有內部或外部稽核程序，以因應客訴、違反個人資料保護或安全措施時？			
遵循性與賠償	組織是否規範有賠償當事人程序，以因應當發生客訴、違反個人資料保護或安全措施時？			
遵循性與賠償	組織是否規範有弱點修補程序，以因應當發生客訴、違反個人資料保護或安全措施時？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
遵循性與賠償	組織是否規範有聯繫執法機構程序，以因應當發生客訴、違反個人資料保護或安全措施時？			
責任	組織是否訂有高階主管及一般員工應遵循之個人資料保護職責？			
責任	組織是否訂有個人資料保護通報和溝通協調程序，以利個人資料保護流程及程序持續改善並遵循法律規範？			
責任	組織是否依據個人資料機密程度進行分級，並建立適當控管程序以確保個人資料受到適當等級之保護？			
責任	組織是否有充足的資源，以實施個人資料保護政策及相關規範？			
責任	組織之個人資料保護管理程序是否已訂定文件化程序並由主管核准實施？			
責任	組織是否有公布個人資料管理程序，包含如何實施作業自我評量以確保其遵循性？			
責任	組織是否有公布個人資料管理程序，包含如何實施外部稽核查核以確保其遵循性？			
責任	組織是否有公布個人資料管理程序，包含如何實施內部稽核查核以確保其遵循性？			
責任	組織是否有公布個人資料管理程序，包含組織參與的外部商業團體會員是否確保其遵循性？			
責任	組織是否有公布個人資料管理程序，包含是否參加個人資料保護之第三方獨立稽核計畫以確保其遵循性？			
責任	組織內部是否對主管、員工及委外廠商實施提升個人資料保護意識計畫？			
責任	組織是否具有個人資料保護基礎架構以適時調整個人資料保護政策及程序之發展(例如：技術變更，法規變更，組織產品 / 服務或營運模式變更)？			
責任	組織是否已建立違反個人資料保護之懲處措施？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
利益	組織是否將個人資料保護的能力及管理框架視為展現可被檢驗之個人資料保護承諾，因此提升忠誠度的優勢？			
利益	組織是否將個人資料保護的能力及管理框架視為經由溝通及展現個人資料保護良善規範，以獲得青睞的優勢？			
利益	組織是否將個人資料保護的能力及管理框架視為組織對違反個人資料保護之情事，具快速應變及恢復營運能力的優勢？			
利益	組織是否將個人資料保護的能力及管理框架視為成為個人資料保護監管機關所示範之優良榜樣的優勢？			
利益	組織是否將個人資料保護納入策略及計畫？			
利益	組織是否以網站標章方式展現其對個人資料保護之承諾及遵循性？			
利益	組織是否以外部稽核及鑑定報告方式展現其對個人資料保護之承諾及遵循性？			
利益	組織是否以高階主管聲明書方式展現其對個人資料保護之承諾及遵循性？			
利益	組織是否考慮成為資訊媒介者或其他保護個人資料機制的機會？			
訓練	組織負責教育訓練的部門是否參加個人資料保護管理相關議題之討論？			
訓練	新進員工報到時，組織是否要求將個人資料保護及公司策略納入新人訓練宣導項目？			
訓練	組織是否將規範個人資料保護遵循議題納入教育訓練計畫？			
訓練	組織對個人資料管理的教育訓練內容是否包含角色及職責之說明？			
訓練	組織對個人資料管理的教育訓練內容是否包含對個人資料的保護政策、實作及程序說明？			

隱私衝擊評估		符合性評估		
風險領域	評估細項	符合	未符合	不適用
訓練	組織對個人資料管理的教育訓練內容是否包含個人資料保護相關議題聯繫窗口說明？			
訓練	組織對個人資料管理的教育訓練內容是否包含如何定期檢討以加強個人資料保護措施的說明？			
訓練	組織個人資料遵循性教育訓練計畫是否包含個人資料蒐集、處理、利用或刪除之管轄範疇？			

資料來源： 本計畫整理

附件5　個資項目個資衝擊分析檢核表

個資項目個資衝擊分析檢核表	負責人：	單位：

1　服務目錄或流程名稱

2　子流程名稱

3　個人資料檔案名稱

4　目前保有多少數量(筆數)的個人資料？

☐ 1-500　☐ 501-5,000　☐ 5,001 – 50,000　☐ 50,000 以上

5　每年大約會處理多少數量(筆數)的個人資料？

☐ 1-500　☐ 501-5,000　☐ 5,001 – 50,000　☐ 50,000 以上

6　每筆資料中包含的個人資料欄位數量為多少？

☐ 1-10　☐ 11-50　☐ 51-100　☐ 100 以上

法源依據與其他規範

個資項目個資衝擊分析檢核表　　負責人：　　單位：

7　組織於蒐集個資前是否主動公告其所依循之法源、機構或合約?

☐ 是　　☐ 否

備註：

8　組織於執行個資蒐集相關業務/專案前是否已完成系統安全計畫？

☐ 是　　☐ 否

備註：

個資相關資訊

9　組織是否使用透過商業廣告方式取得或已公開之個資？

☐ 是　　☐ 否　　☐ 部分　　☐ 不適用

請說明使用這些資料原因與方式與組織如何確認這些個資之正確性?

備註：

10　組織如何確認個資內容之正確性？

說明：

☐ 0. 無確認　　☐ 1. 當面核對相關證明文件

☐ 2. 書面核對相關證明文件　　☐ 3. 與其他來源進行交叉比對

個資之利用

11　組織除執行業務外，是否利用所蒐集之個資進行資料搜尋、分析或統計等用途? 若是，請問這些活動是否已告知當事人? 組織為何需要進行這些活動？

☐ 是　　☐ 否　　☐ 部分　　☐ 不適用

個資項目個資衝擊分析檢核表	負責人：	單位：

備註：

告知

12 前項問題之回應若為是，這些活動是否已告知當事人?

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

說明：

13 當事人是否具有同意、拒絕提供該個資之權利？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

備註：

14 當事人是否具有隨時要求停止蒐集、處理或利用該個資之權利？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

說明：

個資之共享/提供對象

15 組織於個資蒐集之初是否已告知當事人得利用個資之利害相關方與其個資利用方式等相關資訊？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

備註：

16 組織是否限制個資利害相關方利用個資之方式與禁止其從事與原訂個資利用方式無關之活動？

個資項目個資衝擊分析檢核表	負責人：	單位：

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

備註：

個資之更正與補充

17 組織是否有提供當事人查詢或請求閱覽個資或製給複製本？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

說明：

18 組織是否有提供當事人更正或補充其個資？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

說明：

稽核與權責

19 是否定期審視或稽核以確保個資之蒐集、利用及處理皆遵循已訂定之管理規範？

☐ 是 ☐ 否 ☐ 部分 ☐ 不適用

說明：

資料來源： 本計畫整理

附件6　個資項目衝擊分析表

業務或服務作業流程		個人資料檔案名稱	欄位1	欄位2	欄位3	欄位4	欄位5	欄位6	欄位7	欄位8	欄位9	欄位10	欄位11	欄位12	欄位13	欄位14	欄位15	欄位16	欄位17	欄位18
服務目錄或流程名稱	子流程名稱																			

欄位說明：

欄位1：目前保有多少數量(筆數)的個人資料？

欄位2：每年大約會處理多少數量(筆數)的個人資料？

欄位3：每筆資料中包含的個人資料欄位數量為多少？

欄位4：於蒐集個資前是否主動公告其所依循之法源、機構或合約?

欄位 5：法定保存期限

欄位 6：自定保存期限

欄位 7：於執行個資蒐集相關業務/專案前是否已完成系統安全計畫？

欄位 8：是否透過商業廣告方式取得或使用已公開之個資？

欄位 9：如何確認個資內容之正確性？

欄位 10：除執行業務外，是否利用所蒐集之個資進行資料搜尋、分析或統計等用途?

欄位 11：前項問題之回應若為是，這些活動是否已告知當事人?

欄位 12：當事人是否具有同意、拒絕提供個資之權利？

欄位 13：當事人是否具有隨時要求停止蒐集、處理或利用該個資之權利？

欄位 14：於個資蒐集之初是否告知當事人得利用個資之利害關係方與其利用方式等資訊？

欄位 15：是否限制利害相關方利用個資之方式與禁止其從事與原訂利用方式無關之活動？

欄位 16：是否有方式提供當事人查詢或請求閱覽個資或製給複製本？

欄位 17：是否有方式提供當事人更正或補充其個資？

欄位 18：是否定期審視或稽核以確保個資之蒐集、利用及處理皆遵循已訂定之管理規範？

資料來源： 本計畫整理

附件7　資安事故通報與紀錄表範例

機關名稱			表單編號		
提出單位		提出人員		提出日期	
處理單位		處理人員		處理日期	

處理過程紀錄

個資事故識別與紀錄
個資事故發生與發現之日期與時間： 遭受揭露之個資範圍與敘述： 遭受揭露個資之儲存媒體：
個資事故評鑑與分類
影響範圍(包含系統、人員、組織)： 可能影響之當事人範圍與人數：

個資事故通報與應變
是否需(或已)通報主管機關、執法單位或媒體： 是否需向社會大眾公告： 通知個資事故當事人之通報對象、內容、方式及時機：
個資事故診斷與調查
個資事故相關採證程序之紀錄、證據保存方式及負責人員： 個資事故根因分析結果：
矯正與預防行動方案
個資事故之新增控制措施(以避免已遭受揭露之個資遭到再次揭露)：

預計方案完成日期		負責人員	
實際方案完成日期		追蹤人員	
覆核主管		覆核日期	

資料來源： 本計畫整理

附件8　稽核計畫範例

機 關 名 稱	*{OO 機關}*				
計 畫 名 稱	*{OOO 年度 第O 次 OOOO 管理作業稽核計畫}*				
擬 定 部 門		負責人		日　期	

1. 稽核目的

為瞭解*{機關名稱}*對於個人資料保護與管理活動執行情形，依據本機關*{內部稽核管理規定}*執行內部稽核，以確保本機關保有的個人資料檔案落實執行相關保護措施。本計畫將採獨立查核方式，判斷相關保護措施的控制目標、方法、流程及程序是否符合*{個人資料保護法}*、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*之要求。

2. 作業方式

依據*{OO 機關內部稽核管理規定}*，自*{日期}*至*{日期}*為止之書面或電子資料為本次稽核樣本之母體。本次稽核將採用書面與實地查核方式進行。

3. 稽核依據

{個人資料保護法}、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*。

4. 稽核範圍

本次執行之稽核範圍包含*{OO 機關所屬 OO 科、OO 室、OO 中心、OO 股...}*。

5. 稽核時程規劃

詳見 7.稽核時程規劃表。

6. 注意事項

{略...}。

7. 稽核時程規劃表

稽　核　日　期	*{OOO 年 OO 月 OO 日}*		
受 稽 核 單 位	*{OO 機關所屬 OO 科、OO 室、OO 中心、OO 股...}*		
稽核小組成員			
時間	活動說明	稽核人員	地點
{09:00 – 09:20}	*{稽核啟始會議}*		*{OOO}*
{09:20 – 10:30}	*{略...}*	*{OOO}*	*{OOO}*
{10:30 – 12:00}	*{略...}*	*{OOO}*	*{OOO}*
{12:00 – 13:00}	午休		
{13:00 – 14:45}	*{略...}*	*{OOO}*	*{OOO}*
{14:45 – 16:30}	*{略...}*	*{OOO}*	*{OOO}*
{16:30 – 17:00}	*{結束會議}*		*{OOO}*

簽核紀錄

初核人員		日期	
覆核人員		日期	
機關主管		日期	

附件9　稽核查核表範例

稽核日期：_____

稽 核 員：_____　　紀錄編碼：

項　次	評　核　內　容	評 核 結 果	備　　註
1	是否已設置個人資料保護聯絡窗口並對外公告	符合 c　不符合 c	
2	是否已明確訂定個人資料保護專責人員之角色職責	符合 c　不符合 c	
3	機關所保有的個人資料檔案清單內容若有異動，是否每月及時更新	符合 c　不符合 c	
4	是否定期進行所保有個人資料檔案項目之盤點	符合 c　不符合 c	
5	是否已識別所保有個人資料檔案項目之內容，例如保有單位、個人資料欄位、保有目的、類別、保存期限等	符合 c　不符合 c	
6	是否定期進行個人資料檔案之隱私衝擊與風險評估活動並識別出對應之風險層級	符合 c　不符合 c	
7	是否針對不同風險層級之個人資料檔案訂定風險管理計畫或處理程序	符合 c　不符合 c	
8	是否記錄並追蹤風險管理計畫或處理程序之執行狀態	符合 c　不符合 c	
9	是否訂有個人資料事故通報及應變程序	符合 c　不符合 c	
10	個人資料事故通報及應變程序中是否包括當個人資料事故發生時對主管機關與當事人進行通報與告知之時機與方式	符合 c　不符合 c	

項　次	評　核　內　容	評核結果	備　　註
11	個人資料事故通報及應變程序中是否包括對個人資料事故相關紀錄與證據之保存、採證及維護管理方式	符合 c　不符合 c	
12	是否設有專責人員負責相關個人資料事故之通報及應變	符合 c　不符合 c	
13	是否設有專責人員負責當個人資料事故發生後之當事人告知與聯繫服務窗口	符合 c　不符合 c	
14	是否對所有個人資料事故紀錄與改善行動方案進行事後審查	符合 c　不符合 c	
15	除依法得免告知之情形外，個人資料蒐集前是否告知當事人對其個人資料蒐集、處理及利用之特定目的範圍	符合 c　不符合 c	
16	除依法得免告知之情形外，與外部第三者之間傳送或複製個人資料檔案，是否符合個人資料檔案之特定目的並取得當事人之同意	符合 c　不符合 c	
17	除依法得免告知之情形外，特定目的以外之個人資料蒐集、處理及利用，是否取得當事人之單獨書面同意	符合 c　不符合 c	
18	是否明確告知當事人對其個人資料內容，以下得行使之權利及方式：(1)查詢或請求閱覽(2)請求製給複製本(3)請求補充或更正(4)請求停止蒐集、處理或利用(5)請求刪除	符合 c　不符合 c	
19	除依法得免取得當事人同意之情形外，個人資料蒐集前是否已取得當事人書面同意	符合 c　不符合 c	
20	是否以達成特定目的所需之最少個人資料需求，進行個人資料之蒐集、	符合 c　不符合 c	

項　次	評　核　內　容	評核結果	備　　註
	處理及利用		
21	是否訂有正式個人資料蒐集、處理及利用之內部管理程序	符合 c　不符合 c	
22	是否已訂立相關人員對個人資料蒐集、處理及利用之角色權責	符合 c　不符合 c	
23	是否落實個人資料蒐集、處理及利用之內部管理程序並留有紀錄與相關軌跡資料	符合 c　不符合 c	
24	是否保存個人資料蒐集、處理及利用之紀錄與相關軌跡資料至少5年以上	符合 c　不符合 c	
25	是否依據不同角色人員存取個人資料檔案的最少需求，設定適當的個人資料欄位遮蔽/隱碼措施	符合 c　不符合 c	
26	是否於委外合約或相關規範中訂定個人資料蒐集、處理及利用之管理程序要求	符合 c　不符合 c	
27	委外合約之組織與個人是否簽訂保密切結書	符合 c　不符合 c	
28	是否進行委外供應者個人資料蒐集、處理及利用之稽核活動並留有紀錄	符合 c　不符合 c	
29	是否訂有個人資料銷毀處理作業程序	符合 c　不符合 c	
30	是否落實個人資料銷毀處理作業程序並留有紀錄	符合 c　不符合 c	
31	是否保存個人資料銷毀作業紀錄至少5年以上	符合 c　不符合 c	
32	資料安全管理及人員管理(此部份參照 ISMS 相關要求辦理)	符合 c　不符合 c	

項　次	評　核　內　容	評核結果	備　　註
33	是否規劃並執行對所有人員的個人資料保護管理認知宣導活動	符合 c　不符合 c	
34	是否規劃並執行對個人資料保護專責人員的資訊安全與個資隱私保護訓練課程	符合 c　不符合 c	
35	是否依據個人資料檔案之不同風險層級訂定對應之設備安全管理技術控制基準	符合 c　不符合 c	
36	設備安全管理(此部份參照 ISMS 相關要求辦理)	符合 c　不符合 c	
37	資料安全稽核機制(此部份參照 ISMS 相關要求辦理)	符合 c　不符合 c	
38	是否定期舉行個人資料保護與管理之整體審查以指示或核准重大個人資料保護管理事宜、相關持續改善計畫及資源需求等	符合 c　不符合 c	

附件10　稽核紀錄範例

機 關 名 稱	*{OO 機關}*		
稽 核 計 畫	*{OOO 年度 第O 次 OOOO 管理作業稽核計畫}*		
受 稽 單 位			
稽 核 人 員		稽 核 日 期	

稽核紀錄

序號	稽核依據	是否符合要求			稽核發現
		Yes	No	N/A	
1					
2					
3					
4					
5					
6					
7					
8					
{n}					

受稽單位確認欄

受稽單位代表		職稱		日期	

附件11　個資項目技術安全控制措施基準值評估表

個人資料檔案名稱：_____

技術控制措施等級：_____

填寫人：_____

填寫日期：_____

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
技術控制措施類別(1)存取控制機制						
1*				普	是否已建立個資處理授權表	包括加密應用於設備、檔案、紀錄、程式、網域等存取活動
2				普	是否已建立應用層之存取控制	
3				普	是否已依據密碼原則設定密碼	
4				普	是否已啟動逾時未操作之密碼保護設定	例如啟用螢幕保護密碼、連線逾時等
5				普	是否已啟動使用者瀏覽器安全設定	例如限制執行非信任網站之程式碼
6				中	是否已依據風險評鑑與人員職責開放必要之最小權限	包括可執行之應用程式、系統功能、通訊埠、通訊協定及服務；或採用以角色為基礎的存取控制機制
7				中	建議採用資料外洩防護(DLP)工具管理使用者傳送個資或機密資料之行為	DLP: Data Loss Prevention
8				中	建議與外單位交換個資時採用數位版權管理(DRM)工具以限定個別使用者之存取權限	DRM: Digital Right Management，依據個資敏感/機密性決定使用者存取限制，例如列印、郵件轉寄、檔案複製、螢幕畫面擷取等
9				高	是否已採用 DLP 與 DRM 工具	若個資為特種個資，必要時應側錄使用者存取行為，並由指定之高階主管審視或抽核是否有不符合個資規範之行為

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
技術控制措施類別(2)職務區隔						
10				中	是否已依據獨立性原則採用職務區隔	例如負責系統管理者不應同時負責管理系統日誌(log)
11				中	職務區隔 是否已應用於系統管理、程式開發、組態管理、系統測試、網路管理等活動	建議結合存取控制，採用以角色為基礎的存取控制機制
12				中	執行存取控制者是否禁止稽核自身相關工作	
13				中	系統管理角色是否已分開使用管理者帳號，而非全部使用最高權限或僅使用單一帳號	例如系統管理可分為3個部分交由3位同仁負責，則每位應擁有其負責之系統管理權限，而非3位擁有相同系統最高權限，若有輪調或代理之需要，則建議採密碼彌封交由主管負責保管
14				高	Level 等級中之內容是否完全符合	
技術控制措施類別(3)最小權限						
15				中	「職務區隔 」Level 等級中之內容是否完全符合	
技術控制措施類別(4)遠端存取						
16				普	「存取控制機制」Level 等級普之內容是否完全符合	遠端存取管制範圍除與本中心之外部連線外，亦包含使用者於本中心非使用本機登入，而透過虛擬私有網路(VPN)、撥接(dial-up)、寬頻網路(broadband)及無線網路(wireless)連線至本中心資訊系統之存取活動
17				中	本中心是否已建立遠端存取之自動監控措施	確保從遠端連線至本中心資訊系統之活動均符合本中心所訂定之遠端存取政策
18				中	遠端存取是否已使用加密線路	確保傳輸資料之機密性與完整性

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
19				中	建議遠端存取透過 VPN 連線，並採用以下至少一項標準： SSL 或 IPSec VPN(或更高安全等級之 VPN) Triple DES、AES-128 或安全等級更高之加密機制 CHAP、EAP 或安全等級更高之身分識別機制	
20				高	Level 等級中之內容是否完全符合	
技術控制措施類別(5)使用者基礎的協同合作與資訊分享						
21				中	是否已禁止將個資儲存於共享資料夾	
22*				中	權限是否已依據個人、組別、組織等層級進行功能分類與授權	例如限制讀取、寫入、刪除、執行、列印等
23				中	建議使用 DLP 與 DRM 工具	請參閱「存取控制機制」Level 等級中之控制措施
24				中	儲存於資料庫之密碼與敏感/特種個資是否已運用雜湊函數(hash)之輸出值儲存資料	建議採用 MD5 或 SHA-1 或安全等級更高之雜湊演算法
25				高	Level 等級中之內容是否完全符合	
26				高	儲存於資料庫之密碼與敏感/特種個資是否已運用雜湊函數(hash)之輸出值儲存資料	建議採用 SHA-1 雜湊演算法之輸出值儲存
技術控制措施類別(6)可攜式與行動設施的存取控制機制						
27				普	可攜式行動裝置若連接至本中心內部網路與資訊系統時是否已經過授權始可使用	可攜式行動裝置包含外接儲存設備(如 USB 隨身碟、外接硬碟)、含有資料儲存功能之可攜式行動運算/通訊

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
						設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等)
28				普	可攜式行動裝置若連接至本中心內部網路與資訊系統時是否符合本中心資訊安全原則	例如使用這些裝置時應進行必要之組態調整、設備識別碼應提供予裝置管理人員、應依據該申請者職責授權、必要時應安裝某些保護軟體(例如防毒軟體、設定防火牆等)且必要時應更新系統，例如防毒軟體更新至最新定義檔、可攜式裝置更新至原廠提供之最新修補程式
29				普	可攜式行動裝置若連接至本中心內部網路與資訊系統時，申請人是否主動提供可攜式行動裝置予裝置管理人員進行掃描	例如執行系統完整性檢查、移除/停用不必要之硬體/服務(如無線接收、紅外線)
30				普	若人員需要攜出屬於本中心之可攜式裝置(例如出差或外出執行公務等)，回來的時候是否已檢查曾去的地方是否屬於高風險	例如檢查組態設定是否遭到調整、硬碟是否被置換、是否多安裝某些應用程式等
31				中	Level 等級普之內容是否完全符合	
32				中	是否已限制可寫入與可攜式媒體之使用(僅授權人員得使用)	
33				中	是否已禁止使用私有之可攜式媒體	
34				中	是否已禁止無特定保管者之可攜式媒體的使用	
35				中	建議使用 DLP 與 DRM 工具	請參閱「存取控制機制」Level 等級中之控制措施

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
36				高	Level 等級中之內容是否完全符合	
技術控制措施類別(7)稽核事件						
37				中	具有最高或特殊權限之使用者或其授權使用之系統功能是否已設定事件稽核日誌(event log)	
38*				中	是否已指派專人定期審視事件稽核日誌(event log)	為維護事件稽核之獨立性，事件稽核日誌應即時備份至另一獨立主機(如 log server)，且原系統管理者不應具有該 log server 之管理權限
39*				中	若事件稽核日誌包含敏感/特種個資內容，是否已加密處理，僅負責審視或稽核該日誌者得存取完整內容	
40				高	Level 等級中之內容是否完全符合	
技術控制措施類別(8)稽核紀錄的監控、分析及報告						
41*				普	是否已定期執行個資管理稽核活動	確認是否有違反個資安全的異常行為，稽核報告與結果應呈報至相關管理者
42*				普	當發生重大變更時，是否已重新審視個資管理稽核計畫與頻率，並視需要進行調整	重大變更包含資訊資產、組態項目、資產、人員或組織形態有重大變更，或是個人資料保護法條文有異動
43				中	Level 等級普之內容是否完全符合	
44				高	Level 等級中之內容是否完全符合	
45				高	是否已留存資訊系統之分析紀錄與稽核報告	以備於異常事件發生時供本中心相關人員進行調查與回應
技術控制措施類別(9)識別與鑑別(機關使用者）						

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
46				普	使用者帳號是否具有唯一鑑識性	使用者包含本中心正職員工、約聘員工、顧問等
47				普	當使用者群組具有最高權限(如administrator)或特殊權限時，審核者是否已謹慎考量該群組所擁有之所有權限是否與使用者角色/權責相符	可對於具有相同權限之使用者設定存取權限群組，但若該群組具有最高權限(如 administrator)或特殊權限時，審核者應謹慎考量該群組所擁有之所有權限是否與使用者角色/權責相符
48				普	機敏等級為高之系統使用者身分認證是否已採二元識別(two-factor authentication)或多元識別(multifactor authentication)等認證方式	使用者身分認證方式包含使用者帳號、密碼、token、生物辨識(如指紋辨識)，機敏性較高之系統亦可使用二元識別(two-factor authentication)或多元識別(multifactor authentication)等認證方式
49				普	使用者身分識別是否已應用於系統本機端存取(local access)與遠端存取(包含透過 LAN、WAN 或 VPN 等方式)	
50				中	Level 等級普之內容是否完全符合	
51				中	所有使用者透過遠端登入時，是否已使用二元識別或多元識別之認證	
52				中	資訊系統之最高權限或特殊權限使用者於本機登入時，是否已使用二元識別或多元識別之認證	
53				中	資訊系統之最高權限或特殊權限使用者透過遠端登入時，是否採用重送攻擊防阻之認證機	如使用含token動態密碼之二/多元認證或時間戳記(timestamp)認證協定

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
					制(replay resistant authentication)	
54				高	Level 等級中之內容是否完全符合	
55				高	所有使用者無論於本機或遠端登入時，是否已使用二元識別或多元識別之認證	
56				高	所有使用者於遠端登入時，是否已採用重送攻擊防阻之認證機制(replay resistant authentication)	如使用含token動態密碼之二/多元認證或時間戳記(timestamp)認證協定
57				高	傳送電子文件(包含電子郵件)時是否已使用數位簽章	
技術控制措施類別(10)媒體存取						
58*				中	是否已設置具有實體安全控管之環境存放備份媒體，且嚴禁非授權存取備份媒體	資訊系統媒體包含電子媒體(如光碟、磁帶、外接式硬碟、USB隨身碟、記憶卡等)與非電子媒體(如紙本文件、膠卷等)，亦應應用至含有資料儲存功能之可攜式行動運算/通訊設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等)
59				中	建議可使用 DLP 與 DRM 工具	請參閱「存取控制機制」Level 等級中之控制措施
60				高	Level 等級中之內容是否完全符合	
技術控制措施類別(11)媒體標記						
61*				中	個資等級標示範圍是否已包含應用系統與資訊系統媒體	相關定義請參考「媒體存取」控制措施說明
62*				中	建議標示書面文件等級	例如將等級標示於文件封面、封底或以浮水印的方式呈現

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
63				高	Level 等級中之內容是否完全符合	
技術控制措施類別(12)媒體儲存						
64				中	存放儲存個資儲存媒體之場所是否已設有實體管控措施，並限制可接觸該媒體之人員	本控制項應包含資訊系統媒體(相關定義請參考「媒體存取」控制措施說明)、可攜式行動裝置(相關定義請參考「可攜式與行動設施的存取控制機制」控制措施說明)及可儲存資料之電話系統(如留言系統或磁帶)
65				中	個資是否已加密後進行儲存，加密強度依據個資機密和完整性等級設定	
66				高	Level 等級中之內容是否完全符合	
技術控制措施類別(13)媒體運輸						
67*				中	是否已限制負責傳輸或傳送存有個資儲存媒體之人員	本控制項應包含資訊系統媒體、可攜式行動裝置及可儲存資料之電話系統(如留言系統或磁帶)
68*				中	個資儲存媒體於傳送時所使用之包覆措施是否已具有實體管控措施	例如密封盒、可上鎖之儲物箱等
69				中	個資是否已加密後始進行儲存	加密強度應依據個資機密和完整性等級設定
70*				中	個資儲存媒體運送時是否已記錄儲存媒體相關資料	例如儲存媒體識別資料(如磁帶編號)、傳送人員簽名、傳送時間、追蹤碼(若適用)與目的地等紀錄
71*				中	若個資儲存媒體需委外傳送(例如透過郵局、快遞公司等)，是否已加強其包覆措施之強度，並留下相關紀錄	

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
72				高	Level 等級中之內容是否完全符合	
73*				高	是否已指派專人負責遞送個資儲存媒體	
技術控制措施類別(14)媒體淨化						
74*				普	是否已依據個資機敏等級選擇適當的儲存媒體淨化方式	本控制項適用於所有即將淘汰、廢棄或重複使用之個資儲存媒體，個資儲存媒體淨化(Sanitization)方式包含媒體清除(clear)、刪除(purge)及破壞(destory)。 等級普之儲存媒體淨化方式建議如下： ¡ 電子儲存媒體應採用多次亂數覆寫工具(data erasure)以抹除儲存資料 ¡ 非電子儲存媒體則應禁止回收使用，例如含個資之文件應攪碎或透過水銷、焚燒等方式銷毀
75				中	Level 等級普之內容是否完全符合	
76*				中	是否已依據個資機敏等級選擇適當的儲存媒體淨化方式	等級中之儲存媒體淨化方式建議如下： ¡ 將重複使用之電子儲存媒體應採用多次亂數覆寫工具(data erasure)以抹除儲存資料，且應限制僅能提供本中心內部人員使用；將報廢之電子儲存媒體則應採取消磁或實體破壞的方式銷毀 ¡ 非電子儲存媒體則應透過水銷或焚燒方式銷毀
77				高	Level 等級中之內容是否完全符合	
78*				高	是否已追蹤、記錄並核對儲存媒體淨化與銷毀程序	

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
79*				高	是否已定期測試儲存媒體淨化設備與程序是否正常運行	
80				高	是否已於使用資訊系統媒體與可攜式行動裝置前先進行媒體淨化程序	以避免惡意程式感染本中心之資訊系統
81				高	電子儲存媒體若需重複使用是否已採用多次亂數覆寫工具(data erasure)以抹除儲存資料，且僅限於原存取該個資之使用者/群組之人員使用，不得提供其他部門或外部人員使用	
技術控制措施類別(15)傳輸機密性						
82				中	資料傳輸時是否已進行加密，	本控制項適用於透過內部網路、無線網路、外部網路之資料傳輸，應用程式包含 E-mail、FTP 等 建議標準如下： ¡ 應採用 Triple DES、AES-128 或安全等級更高之加密機制 ¡ 應採用 CHAP、EAP 或安全等級更高之身分識別機制 ¡ 若傳輸網路無法加密，則所傳輸之檔案或資料應進行加密，建議使用 128 位元以上進行加密
83				中	使用無線網路時，是否已提供以下設定與限制： 避免使用 SSID 廣播 限制可使用無線網路之無線網卡 MAC 位址	應採用 WPA 或 WPA2 以上認證方式搭配 TKIP、CCMP 或安全等級更高之安全協定
84				高	Level 等級中之內容是否完全符合	
85				高	是否已禁止使用無線網路傳輸等級為高之資料	

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
技術控制措施類別(16)靜態資訊的保護						
86				中	「媒體淨化」Level 等級中之控制措施是否完全符合	本控制項適用於硬碟與儲存媒體
87				高	Level 等級中之內容是否完全符合	
技術控制措施類別(17)資訊系統監視						
88				中	是否已建置可偵測資訊系統攻擊事件之監控與防護工具	監控與防護工具可分為內部和外部，內部包含系統監視、內部網路或系統元件之間的事件偵測工具，外部則包含偵測由外部傳輸進來之封包、資料及附檔等工具，並於偵測到惡意行為時得阻擋或提供即時警示功能之防護工具
89				中	是否已設置防火牆(firewall)協助進行網路監控與防護	
90				中	是否已設置惡意軟體偵測(如防毒軟體、防木馬間諜軟體等)協助進行網路監控與防護	
91				中	是否已設置入侵偵測系統(IDS)或入侵防禦系統(IPS)協助進行網路監控與防護	
92				中	是否已設置電子郵件/網路瀏覽內容安檢軟體(MIMESweeper、Spam filter 等)協助進行網路監控與防護	
93				中	資訊系統監視工具是否已識別未經授權的資訊系統存取活動，並具有即時事件分析功能	
94				中	資訊系統監視工具是否已架設於本中心與外部網路連接界	

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
					限、重要伺服器(server farm) 與內部網路界限	
95				中	組織使用之自動化監測工具是否已具有偵測內送(inbound)與外發(outbound)資料傳輸之異常或非授權之活動或狀況等功能	例如偵測惡意程式或異常大量傳送之封包
96				中	組織使用之自動化監測工具是否已具有提供近乎即時之警訊(alert)功能	當可能造成資訊系統遭受功擊前/時，即時通知相關人員進行處理
97				中	自動化監測工具若需自行設定政策、過濾條件(如 firewall、MIMESweeper 等)，是否已定期檢視相關政策與設定	若由原廠提供定義檔(如防毒軟體、防木馬間諜軟體等)則應即時更新。
98				中	是否已定期執行資訊系統滲透測試與弱點掃描測試	應針對中、高風險(至少)之測試掃描結果進行改善
99				中	自行開發之系統是否已執行原始碼檢測	檢測項目至少包含 OWASP Top 10 等著名安全問題
100				高	Level 等級中之內容是否完全符合	

資料來源： 本計畫整理

附註：項次有*者為紙本之控制措施

附件12　委外作業稽核計畫範例

機 關 名 稱	*{OO 機關}*				
委外單位名稱	*{OO 公司}*				
計 畫 名 稱	*{OOO 年度 第O 次 OOOO 管理委外作業稽核計畫}*				
擬 定 部 門		負責人		日　期	

1.稽核目的

為瞭解*{OO 公司}*對於*{機關名稱}*個人資料委外作業之保護與管理活動執行情形，依據本機關*{內部稽核管理規定}*執行委外廠商稽核，以確保*{OO 公司}*落實本機關對個人資料檔案相關保護措施之要求。本計畫將採獨立查核方式，判斷相關保護措施的控制目標、方法、流程及程序是否符合*{個人資料保護法}*、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*之要求。

2.作業方式

依據*{OO 機關內部稽核管理規定}*，自*{日期}*至*{日期}*為止之書面或電子資料為本次稽核樣本之母體。本次稽核將採用書面與實地查核方式進行。

3.稽核依據

{OO 委外作業案合約}、*{個人資料保護法}*、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*。

4.稽核範圍

本次執行之稽核範圍包含*{OO 公司}*所承接本機關*{OO 委外作業案}*其中合約所規範之個人資料蒐集、處理及利用等相關流程。

5.稽核時程規劃

詳見 7.稽核時程規劃表。

6.注意事項

{略...}。

7.稽核時程規劃表

稽　核　日　期	*{OOO 年 OO 月 OO 日}*		
受 稽 核 單 位	*{OO 公司}*		
稽核小組成員			
時間	活動說明	稽核人員	地點
{09:00 – 09:20}	*{稽核啟始會議}*		*{OOO}*
{09:20 – 10:30}	*{略...}*	*{OOO}*	*{OOO}*
{10:30 – 12:00}	*{略...}*	*{OOO}*	*{OOO}*
{12:00 – 13:00}	午休		
{13:00 – 14:45}	*{略...}*	*{OOO}*	*{OOO}*
{14:45 – 16:30}	*{略...}*	*{OOO}*	*{OOO}*
{16:30 – 17:00}	*{結束會議}*		*{OOO}*

簽核紀錄

初核人員		日期	
覆核人員		日期	
機關主管		日期	

附件13　委外作業稽核紀錄表範例

機 關 名 稱	*{OO 機關}*		
稽 核 計 畫	*{OOO 年度 第O 次 OOOO 管理作業稽核計畫}*		
受 稽 單 位	*{OO 公司}*		
稽 核 人 員		稽 核 日 期	

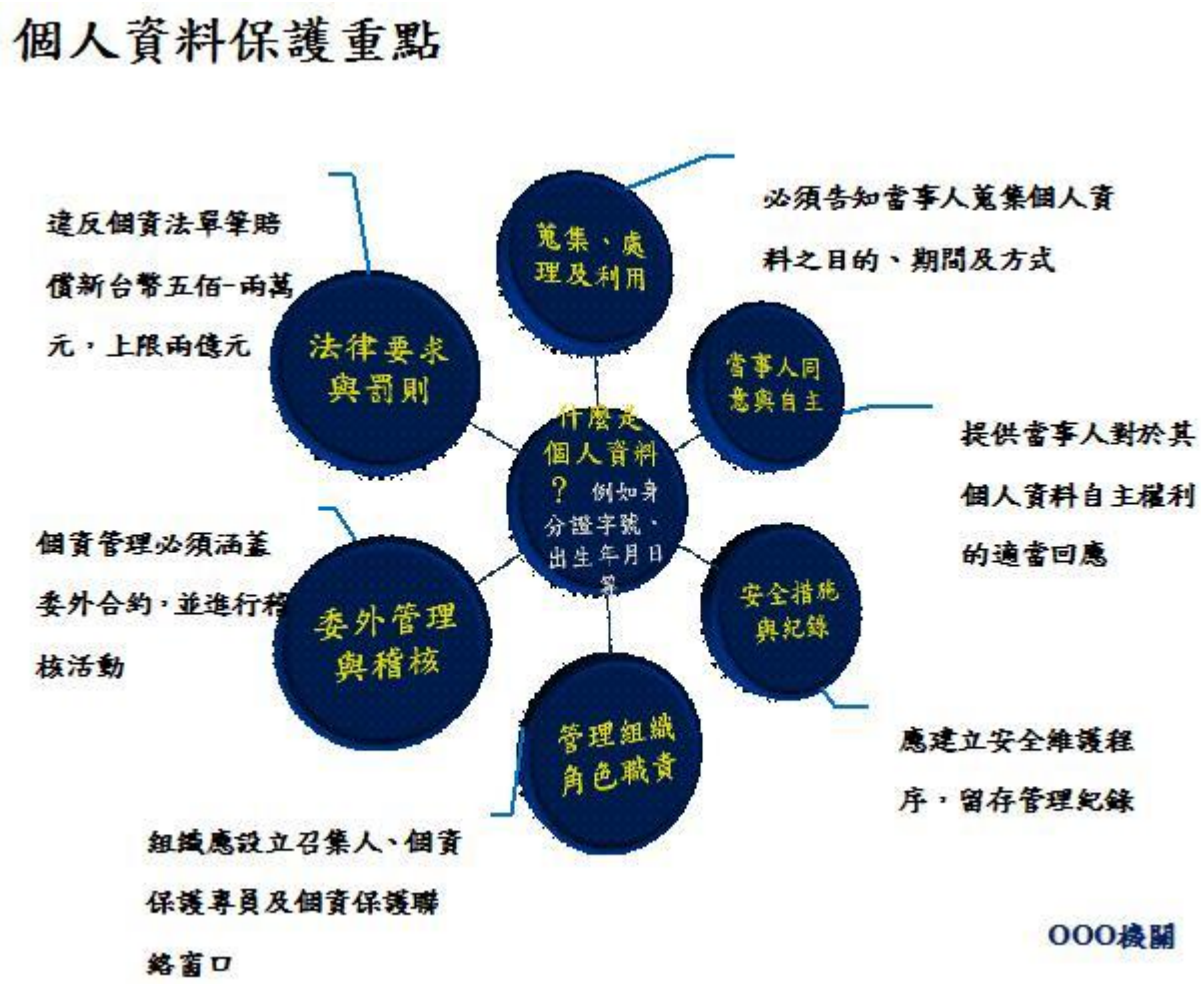
稽核紀錄

序號	稽核依據	是否符合要求			稽核發現
		Yes	No	N/A	
1					
2					
3					
4					
5					
6					
7					
8					
{n}					

受稽單位確認欄

受稽單位代表		職稱		日期	

附件14　個資認知宣導海報範例



附件15　預防與矯正行動方案範例

機關名稱			表單編號		
提出單位		提出人員		提出日期	
處理單位		處理人員		處理日期	

說明

不符合事項/問題來源與說明
根本原因分析
矯正與預防措施說明

預計改善完成日期		負責人員	
實際改善完成日期		追蹤人員	
覆核主管		覆核日期	

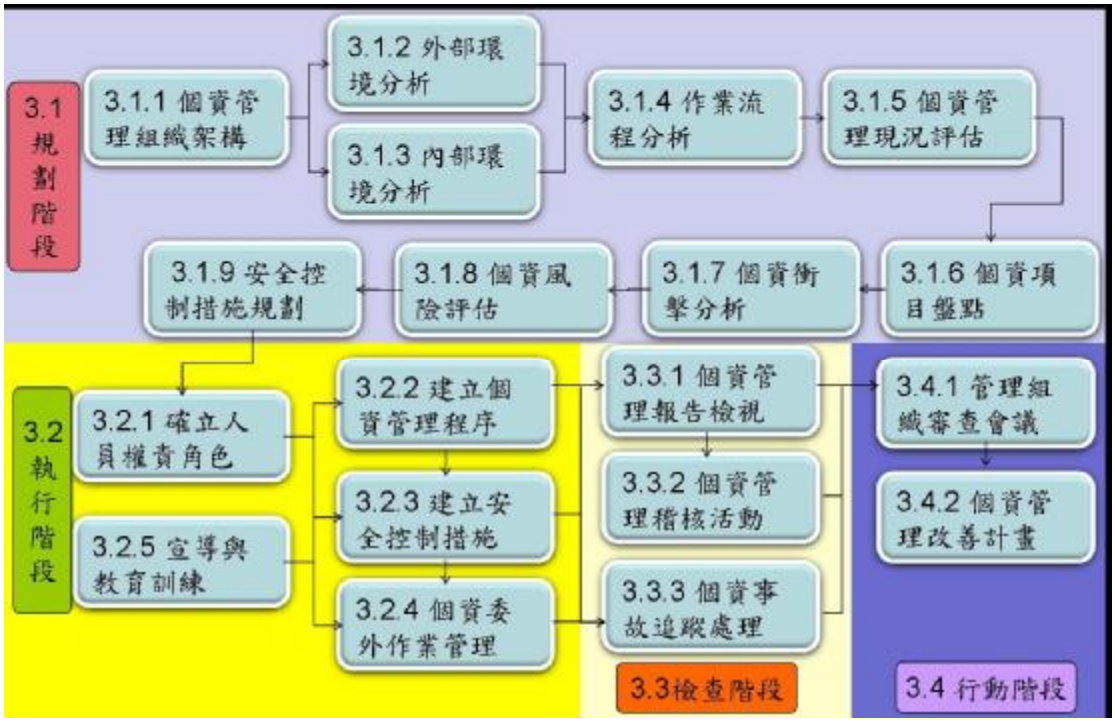
資料來源： 本計畫整理

附件16　個人資料保護參考指引導引手冊(Quick Guide)

個人資料保護參考指引導引手冊

1. 本指引主要依據 99 年度發展之「個資保護規劃與實作建議報告」，並參考國際個人資料保護相關標準(NIST SP800-122、BS 10012 等)，編訂「個人資料保護參考指引」(以下簡稱本指引)，提供政府機關執行個人資料保護相關做為之參考。本指引係屬建議性質，政府機關可參考本指引，就機關特性、業務需求等，以符合個人資料保護法(以下簡稱個資法)與其施行細則、國際隱私保護原則及個資管理標準等相關規定為原則，針對資訊系統與所屬資產進行個人資料保護。

2. 個資保護管理建置流程，在於發展一套適用於政府機關，因應個資法實施時，如何建立個資管理機制之參考。首先須符合我國個資法與其施行細則之法規命令要求，同時能夠與國際隱私保護相關發展趨勢、標準等接軌。據此發展相關建置流程，協助政府機關持續提升個資保護管理。個資保護管理建置流程之整體發展架構，詳見圖 1：



資料來源： 本計畫整理

圖1　個資保護管理建置流程之整體發展架構

3. 建立個資保護管理組織

為展現組織對個資保護的承諾與決心，應成立個資管理組織，由各部門代表參與，並明確界定該組織內相關角色職掌，並且由專人擔任個資保護聯絡窗口，做為統一的個資管理溝通管道。有關建立個資保護管理組織之任務，說明如下：

Ÿ　瞭解組織現行架構(含單位別與功能性)與人員角色職責

可蒐集單位組織圖、管理制度架構圖及角色職責分工定義等相關資料，再配合人員訪談方式，瞭解各部門的作業內容是否與個資相關或持有個資。

Ÿ　定義個資管理組織

應有高層主管擔任召集人，並由跨部門人員(建議由部門主管)參

與。對於已導入 ISMS 的單位，可考量將 ISMS 與個資適當整合成一個管理組織。此外，當個資管理涵蓋範圍超過資訊單位的業管範圍時，建議考量由其他適當部門主辦與協調，進行個資管理活動之推動。

Ÿ 定義個資管理組織人員角色職責

在個資管理組織中，應明確描述各人員的角色與職掌，並建議由個資保護專責人員擔任此功能性組織之溝通協調。該組織人員可包括召集人、個資保護專責人員、個資聯絡窗口、個資保護規劃小組、個資保護應變小組、個資保護文件管制小組及稽核小組等，有關個資管理組織與角色職責分工範例詳見表 1；詳細內容請參考本指引 3.1.1 與 4.1 章節。

表 1 個資管理組織與角色職責分工範例

組織架構角色	工作職掌
召集人	▪擔任個資與隱私保護之召集人，統籌決策及組織資訊安全與個資與隱私保護管理業務之資源整合運用 ▪每年審核並頒行個資保護與隱私政策 ▪指派個資管理推動組織架構所需之角色人員，如個資保護專員、個資保護聯絡窗口、資訊服務管理組個資保護工作組長等 ▪核定個資管理文件的制定、修訂及廢止 ▪定期或不定期審核個資與隱私保護計畫 ▪審核內部稽核之稽核計畫與稽核報告 ▪審核個資管理推動所須之資源及計畫，並編列相關預算，如人員任用及教育訓練計畫等
個資保護專責人員	▪協助召集人推行個資管理 ▪依相關法規命令辦理安全維護及保管事項 ▪傳達召集人之決策，以貫徹個資管理 ▪協調各組使組織相關個資保護之運作更落實

組織架構角色	工作職掌
	▪彙集、轉陳各組之意見、資料，供召集人做最佳決策 ▪協助追蹤、管理個資保護稽核所提相關建議事項 ▪定期蒐集、分析及陳報個資相關通報及執行狀況之報告
個資聯絡窗口	▪機關對外之個人資料保護業務聯繫協調 ▪個人資料安全事故通報 ▪重大個人資料外洩事件單一聯繫窗口 ▪接受與回覆當事人依法提出個人資料權利之請求事宜
個資保護規劃小組	▪協助召集人與個資保護專責人員推行執行個資管理活動 ▪傳達召集人之決策，以貫徹個資管理 ▪執行各組工作使相關個資保護之運作更落實 ▪轉陳各組之意見、資料予個資保護專員彙整供召集人進行決策 ▪協助追蹤、管理個資保護稽核所提相關建議事項 ▪定期蒐集、分析及陳報個資相關通報及執行狀況之報告
個資保護應變小組	▪個人資料事故處理與應變相關資源之規劃與取得 ▪個人資料事故通報、處理及應變相關活動內外部聯繫與協調 ▪個人資料事故證據之保存、鑑識及調查分析 ▪個人資料事故之公關與客服處理 ▪個人資料事故通報、處理及應變相關活動之教育訓練與演練 ▪個人資料事故通報、處理及應變目標與程序之持續改善提升
個資保護文件管制小組	核定之個資保護文件登錄、發行、保存等相關管理工作

組織架構角色	工作職掌
各單位專責人員	▪ 落實個資與隱私保護相關作業規範 ▪ 配合執行或參加個資與隱私保護相關教育訓練 ▪ 執行管理階層於個資與隱私保護之決策及交辦事項 ▪ 配合召集人或所授權人員執行風險審查包括： – 鑑別與盤點單位之個資項目 – 鑑別個資項目潛在風險與提出需求 – 鑑別個資項目所須之安控機制 – 各類隱私事故之報告與處理 – 參與並推廣個資管理與隱私保護觀念教育訓練
委外廠商與相關人員	▪ 遵循組織制定之個資保護與隱私政策與相關作業規範 ▪ 配合組織辦理之個資與隱私保護管理稽核活動
稽核小組	▪ 研提年度個資與隱私保護管理稽核計畫 ▪ 配合年度稽核計畫執行相關稽核活動並提供改善建議事項予召集人

資料來源： 本計畫整理

4. 個資項目盤點

個資項目盤點主要目的在盤點組織所擁有之個資項目內容，包括個資項目的類別、目的、來源、欄位、數量、型態、相關生命週期活動、相關利害關係人等，以利後續進行個資之個資衝擊分析、個資風險評估、保護及管理等活動。有關個資項目盤點之任務，說明如下：

Ÿ 識別不同作業流程之個資項目

進行個資盤點時，首先分析服務目錄與服務等級協議中，各服務內容之作業流程與應用系統清單，並經由訪談方式識別含個資之業務或服務作業流程，填註於個資流程分析表。

Ÿ 識別個資項目之類別、依據及目的

組織應將識別出之個資項目，依個資法與其施行細則所規定之個資管理應完成事項清單、行政命令、準則，識別個資項目之蒐集範圍、類別、蒐集依據及蒐集目的，做為未來通知利害相關人之依據。

Ÿ 識別個資項目相關生命週期活動

個資法對於個資管理相關活動分為蒐集、處理、利用及國際傳輸等階段，分別定義如下：

蒐集：指以任何方式取得個人資料。

處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

利用：指將蒐集之個人資料為處理以外之使用。

國際傳輸：指將個人資料作跨國（境）之處理或利用。

另參考 ISO/IEC 29100 隱私框架，對於個資提供者與接收者之間，從個資的蒐集到銷毀階段，可分為數個細部階段，其中特將銷毀階段納入考量，建議政府機關除考量個資法對於個資管理相關活動外，宜將刪除或銷毀納入考量。

Ÿ 識別個資項目與外部利害關係人之關聯

個資與隱私保護之利害關係人包括當事人、組織內部人員、委外人員、供應者及其他可能接觸到組織所屬個資之相關人員。本階段主要就個資項目盤點結果所識別出之個資項目，清查其與外部利害關係人在其不同生命週期的型態、相關文件、支援系統及彼此間之關聯，以做為建立委外管理控制之依據。

Ÿ 完成個資項目盤點

綜整個資項目基本資料與利害關係人，完成個資項目盤點，做為後續個資衝擊分析與個資風險評估之依據；詳細內容請參考本指引 3.1.6 與 4.2 章節。

5. 個資項目衝擊分析

個資衝擊分析的主要目的，在於瞭解個資在蒐集、處理及利用過程中，是否已符合組織所處環境的法規命令與個資保護政策等遵循性要求。有關個資衝擊分析之任務，說明如下：

Ÿ 設計個資衝擊分析檢核表

個資衝擊分析檢核表主要就個資在蒐集、處理及利用過程中，是否提供當事人相關權利(如查詢、閱覽及複製等)與定期審視個資保護管理措施等機制，設計檢核表。

Ÿ 進行個資項目個資衝擊分析

組織應依據個資項目盤點所完成之個人資料檔案名稱，各別填寫個資項目個資衝擊分析檢核表，並彙整所有檢核表內容至個資項目衝擊分析表。

Ÿ 完成個資衝擊分析

組織應依據上述個資項目衝擊分析表，討論相關改善方式，並撰寫個資衝擊分析報告，做為未來改善計畫之依據；詳細內容請參考本指引 3.1.7 與 4.3 章節。

6. 個資風險評估

個資風險評估係針對組織所擁有個資項目的機密性、完整性及可用性等構面向，進行個資風險評估作業，以瞭解個資項目之風險

等級，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。有關個資風險評估之任務，說明如下：

Ÿ 設計個資項目之個資風險等級基準值

組織應依個資流程分析，藉由設計問卷與實地訪談，確認組織存在那些個資項目，以及這些項目是以何種形式存在(是以系統或者表單存在)與擁有之個資類別 (如一般個資或特種個資)。

另組織應就法律層面上洩露不同類別與數量個資時的違法性風險、保護可識別之個資的機密性、資訊資產之影響構面等，設計個資風險等級基準值。基準值設計可依據含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式及「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應等 3 個層面。含有個資類別係以在法律層面上，洩露不同類別與數量個資時的違法性風險，政府機關應依個資洩露筆數所造成之風險程度不同，以及個資法對於不當揭露個資時，在法律責任上之每筆賠償金額，訂定適當筆數做為數量之級距建議。在 NIST SP800-122「個人可識別資訊保護指引」之衝擊等級判定方式，係參考美國 NIST SP800-122(Guide to Protecting the Confidentiality of Personally Identifiable Information)做為技術性控制措施，該文件主要提供以風險為基礎的方法與指導方針，來協助保護可識別之個人資料的機密性。「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應，係依據行政院國家資通安全會報(以下簡稱「資安會報」)所頒「資訊系統分類分級與鑑別機制」參考手冊之資訊資產之影響構面等級，進行對個資項目價值之對應。

Ÿ 分析個資項目個資性之風險等級

每個個資項目應依個資風險等級基準值建議，就其含有個資類

別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式及「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應等 3 個層面之個資風險等級，填註 PIA/RA 安全控制項目基準值。

Ÿ 完成個資風險評估

個資風險等級評估，係依據 PIA/RA 安全控制項目基準值之組織含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式及「資訊系統分類分級與識別機制」影響構面與個資項目價值進行對應，採最高原則方式判別，填註個資項目個資風險評估表，主要區分為普、中、高。例如在個資類別評等為”中”，在 NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級評等為”普”，在「資訊系統分類分級與識別機制」影響構面評等為”高”，則其個資風險等級採最高原則應為”高”。

依所述之判定原則，評估每個個資項目之風險等級，即完成個資項目個資風險評估表內容，以做為檢討安全控制措施規劃之依據；詳細內容請參考本指引 3.1.8 與 4.3 章節。

7. 個資人員權責角色訂定

在處理個資時，需確認組織內外及相關人員之權責角色，並依照其權責給予所應具備之權限，在發生個資事故時，便可儘速釐清可能洩露之管道。有關個資人員權責角色訂定之任務，說明如下：

Ÿ 識別個資管理相關人員或群組角色

針對各單位之工作內容與特性，應瞭解在個資處理過程中，有那些角色、人員及系統使用權限，釐清其相互關係，包括內部/外部使用者、管理者及供應商。

Ÿ 建立個資項目生命週期活動與個資管理角色之對應表

依據個資檔案名稱與識別之個資管理角色，列出各管理者之個資使用情形，包括蒐集、建立、讀取、更新、列印、刪除及轉出等，並將上述資料填入個資項目與個資管理角色對應表。

Ÿ 識別對應表內個資管理角色細部權責定義需求

根據已完成之個資項目與個資管理角色對應表，與各單位進行訪談，瞭解其角色與權限是否符合最小權限原則。

Ÿ 完成人員權責角色定義

依照與各單位訪談結果，調整個資項目與個資管理角色對應表。

Ÿ 轉換個資管理人員權責角色定義至相關應用系統權限定義

完成個資項目與個資管理角色對應表，依其權責角色修正系統或檔案使用權限。以組織現行業務，填寫個資項目與個資管理角色對應表。實務情形若有涉及代理人，則應詳列代理人之權限；詳細內容請參考本指引 3.2.1 與 4.4 章節。

8. 個資安控措施評估

依據個資法、組織內部法規、主管機關規定及內部個資管理政策，建置個資管理安全控制措施，以降低個資外洩之風險，符合組織內外部規範之需求。有關個資安控制措施評估之任務，說明如下：

Ÿ 分析個資保護技術安全控制項目基準值需求

依個資風險評估報告與個資保護技術安全控制項目基準值建議表，建立個資保護技術安全控制項目基準值需求。個資保護技術安全控制項目基準值，需符合組織所有管理措施要求。

Ÿ 規劃個資生命週期保護構面控制項目行動方案

依個資保護安全控制項目需求與組織經費預算，規劃個資生命週期保護構面控制項目行動方案。

Ÿ 規劃整體環境身分識別與存取管理構面控制項目行動方案

依個資保護安全控制項目需求與組織經費預算，規劃整體環境身分識別與存取管理構面控制項目行動方案。

Ÿ 規劃基礎設施網路安全管理構面控制項目行動方案

依個資保護安全控制項目需求與組織經費預算，規劃基礎設施網路安全管理構面控制項目行動方案。以上三項行動方案之規劃，可同時進行。

Ÿ 建置個資保護安全控制項目行動方案

依據已規劃之行動方案，依時程與預算規劃，執行各項防護措施；詳細內容請參考本指引 3.2.3 與 4.5 章節。

9. 個資委外管理

委外作業雖是由外部第三方執行，但仍需符合組織個資防護要求，故於委外作業流程中，應檢視並要求第三方於處理個資作業時，必須具備個資安全保護措施，同時保留稽核之權利。有關個資委外管理之任務，說明如下：

Ÿ 檢視個資委外作業契約與範圍

依據委外項目與內容，盤點或推估其所涉及個資項目與內容，同時依據組織內之個資管理政策與程序，檢視現有契約內容之符合情形。

Ÿ 調整個資委外作業契約與工作計畫書內容

於工作計畫書中說明廠商需配合組織之個資管理程序，提供個資

相關防護措施，同時需於契約中載明其權利與義務。

Ÿ 規劃個資委外作業稽核計畫

依據委外工作計畫書、契約及組織內部稽核計畫，規劃個資委外作業之稽核計畫。

Ÿ 執行個資委外作業稽核

依個資委外作業之稽核計畫，執行實地稽核作業，蒐集個資管理紀錄；並依據稽核結果，執行必要之改善措施。

第三方(委外)作業之管理，是個資管理流程中需要被特別重視的環節之一，從政府機關的角度考量，個資法中對於公務機關進行委外作業的個資保護職責，屬於公務機關應負的責任範圍，因此，需在委外契約中，明確定義第三方對個資管理上的職責要求和對第三方實施個資管理稽核的權利，以確認委外廠商是否落實相關個資管理作業，以符合個資法對公務機關委外管理之要求。個資作業委外時，應依據該個資項目之衝擊評鑑結果等級，對應個資保護技術安全控制項目基準值需求，列入委外契約中，並註明供應者應不低於基準值之明確安全保護措施。

同時，於契約中註明組織可依此對委外供應者，執行定期或不定期之個資管理稽核活動，以確保供應者落實相關個資保護作業。組織依業務需求，訂定委外契約之個資保護條款與保密切結書，係以組織對委外廠商作業責任之角度擬定；詳細內容請參考本指引 3.2.4 與 4.6 章節。

10.個資宣導與教育訓練

依個資管理之目標與需求，建立並實施個資管理相關人員訓練計畫，以確保組織所有人員能夠認知其在處理個資時的職責。有關

個資宣導與教育訓練之任務，說明如下：

Ÿ 規劃個資認知宣導活動

依據個資政策、個資相關管理制度文件及個人於處理個資所應賦予之責任，辦理認知相關宣導活動，包括會議、網站、海報及公文傳送等方式，執行之各種個資認知活動。

Ÿ 規劃個資管理認知與教育訓練計畫

依個資管理程序、安全控制措施、委外作業及稽核計畫，訂定年度個資管理認知與訓練計畫。

Ÿ 執行個資管理認知與教育訓練計畫

依據年度個資管理認知與訓練計畫，執行相關訓練活動，並定期檢討出席情形與訓練成效，以做為修正訓練計畫之參考；詳細內容請參考本指引 3.2.5 與 4.7 章節。

11.個資管理審查

管理者為掌握個資管理成效，可於管理審查會議中，瞭解目前執行之個資管控措施是否符合外部法規命令要求與內部防護需求，同時檢討整體個資管理之執行成效。有關個資管理審查之任務，說明如下：

Ÿ 彙整外部最新個資相關法規命令

彙整個資法與其施行細則、主管機關要求之個資相關行政命令、組織內自行訂定之個資相關規範，以瞭解目前政策與個資相關管理程序，是否足以涵蓋各項法規命令之要求。

Ÿ 彙整個資管理預防與矯正行動方案

本項內容包括本指引 3.3.1「個資管理報告檢視」活動之第六項任

務「研擬差異項目之預防與矯正行動方案建議」、3.3.2「個資管理稽核活動」活動之第六項任務「研擬預防與矯正行動方案建議」及 3.3.3「個資事故追蹤處理」活動之第四項任務「擬定個資管理新增控制措施建議」，以上三項任務均會產出預防與矯正行動方案；同時為管理審查會議之輸入項目。

- 彙整個資事故追蹤處理結果

本項內容與「個資管理報告檢視」活動之第一項任務「彙整前一檢視週期個資事故紀錄」相關，該任務之產出項目「個資事故通報與處理紀錄彙整」，同時為管理審查會議之輸入項目。

- 彙整內部與個資委外作業稽核結果

將個資相關稽核活動，包括組織內部個資稽核、主管機關執行之個資稽核、委外作業個資稽核，或由第三方執行之個資稽核，彙整所有個資相關稽核結果。

- 舉行管理組織審查會議

以上四項任務所提供之報告或彙整資料，均需列入管理審查會議之議程，使管理階層瞭解個資防護之執行情形，掌握政策目標是否均已付諸於實行。如有未達目標或需改善之情形，則需於會議中討論並做成決議，持續與新增預防與矯正行動方案，同時提供必要之資源，整併為個資管理改善計畫；詳細內容請參考本指引 3.4.1 與 4.8 章節。

12.個資管理改善

依照各項個資管理會議、稽核活動或法規命令，實施個資改善計畫，同時應配置適當之人力與物力之資源，以協助計畫順利執行。有關個資管理改善之任務，說明如下：

Ÿ 安排個資管理改善計畫相關人力與資源

依據個資管理改善計畫，分配所應參與之人力、設備或其他資源及執行時程，因該計畫可能需由不同單位人員共同執行，故需先行溝通需支援之事項與時程，並使參與人員瞭解其任務。

Ÿ 執行個資管理改善計畫

依個資管理改善計畫，執行各項改善措施。

Ÿ 檢視個資管理改善計畫執行結果

定期檢視個資管理改善計畫執行情形，並召開會議瞭解執行進度與窒礙難行狀況，維護計畫如期如質的產出各項改善措施；詳細內容請參考本指引 3.4.2 與 4.9 章節。