行政院研究發展考核委員會
Research, Development and Evaluation Commission, Executive Yuan

【內部使用】

文件編號：ICST-C-019

100年度
國家資通安全技術服務與防護管理委外服務案
個人資料保護參考指引
(V1.0)

執行單位：財團法人資訊工業策進會

中華民國100年12月

報告摘要

報告名稱	個人資料保護參考指引
資訊等級	¨機密　¨密　þ內部使用　¨普通
相關撰稿人	江衍勳、林子群、盧玲朱
閱讀對象	þ一般主管　þ資安人員　þ資訊人員　þ一般使用者

內容摘要：

本報告主要目的係依據 99 年度發展之「個資保護規劃與實作建議報告」，並參考國際個資保護相關標準(如 NIST SP800-122、BS 10012 等)，編訂「個人資料保護參考指引」，以資通安全角度，提供政府機關執行個資保護相關作業之參考。

本指引共分為前言、文獻探討、個資保護管理建置流程、個資保護管理建置實務、結論及參考文獻共 6 部分。第 1 章說明本指引之目的、適用對象、使用建議及指引章節架構介紹；第 2 章說明與本指引相關文獻探討，包括國際個資相關規範與我國個資相關規範；第 3 章介紹本指引建置流程之 4 個階段，分別為「3.1 規劃」、「3.2 執行」、「3.3 檢查」及「3.4 行動」；第 4 章則透過情境範例，引導政府機關依據個資保護管理建置流程之參考步驟，逐步建立機關之個資保護管理制度；第 5 章說明本指引之結論；第 6 章參考文獻則詳列本指引所參考的文件或資料。另於第 3 章部分階段提供範例，供政府機關在導入個資保護之參考。惟政府機關於導入個資保護管理建置流程時，應依據機關之特性、業務需求等予以調整，以符相關法規命令。

關鍵詞	個人資料、個人資料保護法、個資保護管理建置流程

目　次

圖　目　次

表　目　次

1. 前言

1.1.目的

本報告主要依據 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)，以資通安全角度，提供政府機關執行個人資料保護相關作業之參考。**本指引屬建議性質，政府機關可參考本指引，並依據個人資料保護法(以下簡稱個資法)與施行細則、國際隱私保護原則及個資管理標準等，針對機關特性、業務需求等，進行個人資料保護相關作業**。有關個人資料保護法所提之個人資料蒐集、處理及利用之活動，本指引將於建置流程中說明其管理重點與作業流程。

1.2.適用對象

本指引適用於政府機關負責個人資料保護業務相關人員，為便於閱讀與使用，特將適用對象區分為「一般主管」、「資訊人員」、「資安人員」及「一般使用者」，並針對不同對象建議閱讀之重點，詳見表 1。

表1　個人資料保護參考指引適用對象對照表

章	節	款	一般主管	資訊人員	資安人員	一般使用者
2 文獻探討	2.1 個資的定義	2.1.1 個人資料	○	○	○	○
		2.1.2 特種個人資料	○	○	○	○
	2.2 國際個資相關規範	2.2.1 APEC 隱私保護綱領	○	○	○	Δ
		2.2.2 OECD 隱私保護及個人資料之國際傳遞指導方針	○	○	○	Δ
		2.2.3 ISO/IEC 29100 隱私框架 (Information technology-Security techniques-Privacy framework)	○	○	○	Δ
		2.2.4 ISO 22307 金融服務 - 隱私衝擊分析(ISO 22307 Financial services-Privacy impact assessment)	○	○	○	Δ
		2.2.5 BS 10012 資料保護-個資管理系統規格(BS 10012:2009 Data protection-Specification for a Personal Information Management System)	○	○	○	Δ
		2.2.6 NIST SP800-122	○	○	○	Δ
	2.3 我國個資相關規範	2.3.1 個資法修正重點	○	Δ	○	Δ
		2.3.2 對政府機關之衝擊	○	Δ	○	Δ
		2.3.3 政府機關應注意事項	○	Δ	○	Δ
		2.3.4 政府機關應立即研辦事項	○	Δ	○	Δ
		2.3.5 正式施行期程	○	Δ	○	Δ
3	3.1 規劃	3.1.1 個資管理組織架構	○	○	○	Δ

章	節	款	一般主管	資訊人員	資安人員	一般使用者
個資保護管理建置流程		3.1.2 外部環境分析	○	○	○	Δ
		3.1.3 內部環境分析	○	○	○	Δ
		3.1.4 作業流程分析	○	○	○	Δ
		3.1.5 個資管理現況評估	○	○	○	Δ
		3.1.6 個資項目盤點	○	○	○	Δ
		3.1.7 個資衝擊分析	Δ	○	○	Δ
		3.1.8 個資風險評估	Δ	○	○	Δ
		3.1.9 安全控制措施規劃	○	○	○	Δ
	3.2 執行	3.2.1 確立人員權責角色	Δ	○	○	
		3.2.2 建立個資管理程序	Δ	○	○	
		3.2.3 建立安全控制措施	Δ	○	○	
		3.2.4 個資委外作業管理	Δ	○	○	
		3.2.5 宣導與教育訓練	Δ	○	○	
	3.3 檢查	3.3.1 個資管理報告檢視	Δ	○	○	
		3.3.2 個資管理稽核活動	Δ	○	○	
		3.3.3 個資事故追蹤處理	Δ	○	○	
	3.4 行動	3.4.1 管理組織審查會議	○	○	○	
		3.4.2 個資管理改善計畫	○	○	○	
4 個資保護管理建置	4.1 建立個資保護管理組織		○	○	○	Δ
	4.2 個資項目盤點		○	○	○	Δ
	4.3 個資項目衝擊分析與個資項目衝擊評鑑		Δ	○	○	Δ
	4.4 個資人員權責角色訂定		Δ	○	○	
	4.5 個資安控措施評估		Δ	○	○	
	4.6 個資委外管理		Δ	○	○	
	4.7 個資宣導與教育訓練		Δ	○	○	
	4.8 個資管理審查		○	○	○	

章	節	款	一般主管	資訊人員	資安人員	一般使用者
實務	4.9 個資管理改善		○	○	○	
附記	各項符號代表意義說明如下： ○：詳閱 ； △：參考					

資料來源： 本計畫整理

1.3.章節架構

本指引共分為前言、文獻探討、個資保護管理建置流程、個資保護管理建置範例、結論及參考文獻 6 部分進行撰寫，重點摘錄如下：

第 1 章說明本指引之目的、適用對象、使用建議及指引章節架構介紹；第 2 章說明與本指引相關之文獻探討，包括國際個資相關規範，如：APEC 隱私保護綱領、OECD 隱私保護及個人資料之國際傳遞指導方針、ISO/IEC 29100 隱私框架、ISO 22307 金融服務-隱私衝擊分析、BS 10012 資料保護、NIST SP800-122 個人可識別資訊機密性保護指引（以下簡稱 NIST SP800-122）等，我國個資相關規範則說明個資法修正重點、對政府機關之衝擊與應注意事項等；第 3 章介紹本指引建置流程之 4 個階段，分別為「3.1 規劃」、「3.2 執行」、「3.3 檢查」及「3.4 行動」；第 4 章則透過情境範例，引導政府機關依據個資保護管理建置流程之參考步驟，逐步建立機關之個資保護管理制度；第 5 章為本指引之結論；第 6 章參考文獻則詳列本指引所參考的文件或資料。

1.4.使用建議

政府機關如欲瞭解國際在個資與隱私保護相關作法，可參閱 2.2 節國際相關個資規範；如欲瞭解我國個資法修正重點與頒布後應注意事項，可參閱 2.3 節我國個資相關規範。此外，法務部亦委託財團法人資訊工業策進會訂定

「公務機關個人資料保護執行程序暨考核作業手冊」(以下簡稱考核作業手冊)，提供政府機關建立個資保護及管理標準作業化程序，同時加強機關內部考核程序及導入外部監督機制之參考。依照個資法施行細則第 12 條之 11 項安全維護措施，本指引與考核作業手冊之對照關係(詳見表 2)，各機關於執行個資保護時，可視實際需求，在有效控制及符合法令規定情形下，選擇適合的表單、程序及安全控制措施調整運用。

表2　個資法施行細則安全維護措施對照表

個資法施行細則安全維護措施	公務機關個人資料保護執行程序暨考核作業手冊	個人資料保護參考指引
一、配置管理之人員及相當資源	步驟一、訂定個人資料保護管理政策 步驟二、成立個人資料保護管理執行小組 步驟三、製作建置個人資料保護管理制度作業時程表及建置範圍 步驟四、機關公告個人資料保護管理政策 步驟八、配置相當資源	3.1.1 個資管理組織架構 －定義個資管理組織 －建立個資管理政策與要點 －發布個資管理組織架構 3.1.9 安全控制措施規劃 －評估所需資源
二、界定個人資料之範圍	步驟五、盤點法規以及上級機關訂定之規範 步驟六、盤點個人資料	3.1.2 外部環境分析 －瞭解個資管理相關法規命令之遵循需求 －瞭解個資管理相關國際標準、原則等之遵循需求 3.1.4 作業流程分析 －定義和個資相關之流程與應用系統範圍

個資法施行細則安全維護措施	公務機關個人資料保護執行程序暨考核作業手冊	個人資料保護參考指引
		3.1.6 個資項目盤點
三、個人資料之風險評估及管理機制	步驟七、進行個人資料風險評估並擬定風險對策	3.1.7 個資衝擊分析 3.1.8 個資風險評估 3.2.2.建立個資管理程序
四、事故之預防、通報及應變機制	步驟九、訂定個人資料保護管理制度之內部規範	3.3.3.個資事故追蹤處理
五、個人資料蒐集、處理及利用之內部管理程序	步驟九、訂定個人資料保護管理制度之內部規範 步驟十一、開始運作個人資料保護管理制度	3.2.2.建立個資管理程序
六、資料安全管理及人員管理	步驟九、訂定個人資料保護管理制度之內部規範	3.2.1.確立人員權責角色 3.1.9.安全控制措施規劃 3.2.3.建立安全控制措施
七、認知宣導及教育訓練	步驟十、教育訓練	3.2.5.宣導與教育訓練
八、設備安全管理	步驟九、訂定個人資料保護管理制度之內部規範	3.1.9.安全控制措施規劃 3.2.3.建立安全控制措施
九、資料安全稽核機制	步驟十二、檢視個資保護管理制度之運作情形進行改善	3.3.2.個資管理稽核活動
十、使用紀錄、軌跡資料及證據之保存	步驟九、訂定個人資料保護管理制度之內部規範	3.1.9.安全控制措施規劃 3.2.3.建立安全控制措施
十一、個人資料安全維護之整體持續改善	步驟十三、修正個人資料保護管理制度並實施改善措施	3.4.2.個資管理改善計畫

資料來源： 本計畫整理

本指引主要以資通安全角度，探討個資保護管理建置流程，提供政府機關導入個人資料保護系統之參考。請參閱附件 1「個資保護管理建置流程檢核表」，以檢視各階段作業或所擬之文件內容。針對已通過 CNS/ISO/IEC 27001 資訊安全管理系統驗證的機關，建議可考量將個人資料保護納入資訊安全管理系統驗證範圍，並強化個人資料管理相關措施，請參閱 3.5 節說明。

2. 文獻探討

隨著網際網路的快速發展，各種網路應用服務如雨後春筍般出現，如社群網站、電子商務網站、網路拍賣及網路銀行等，這些網路應用服務大多涉及個人資料，一旦安全控制措施不夠完備，容易造成個人隱私資料遭受侵害，國際組織如經濟合作暨發展組織(OECD)、亞太經濟合作組織(APEC)等，均已訂定相關規範，提供其會員國對於涉及個人隱私資料保護問題之處理原則。此外，亦訂定資訊科技-安全技術之個人資料隱私衝擊分析（如 ISO/IEC 29100、ISO 22307 等）、個資管理系統規格（如 BS 10012 等）、個資安全控制措施保護實作（如 NIST SP800-122 等）等個資保護標準及規範。而我國亦於 99 年 5 月 26 日公布「個人資料保護法」，藉以規範個人資料的蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，以下將針對上述的規範、標準及法令等進行說明。

2.1.個人資料的定義(依據「個人資料保護法」)

2.1.1. 個人資料

個人資料(以下簡稱個資)，指任何關於可識別個人或足資識別該個人之資料。指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

2.1.2. 特種個人資料

特種個人資料(以下簡稱特種個資)，包括個人資料中有關醫療、基因、性生活、健康檢查及犯罪前科等內容，特種個資除符合我國個資法中所列之特定情形外，不得蒐集、處理或利用(病歷納入特種個資待修法通過)。

2.2.國際個資相關規範

2.2.1. APEC 隱私保護綱領

亞太經濟合作會議(Asia-Pacific Economic Cooperation, APEC)「隱私保護綱領(Privacy Framework)」緣起於 APEC 1998 年電子商務行動計畫，要實踐電子商務相關技術與政策，必須建立安全、保密且可信賴的通訊、資訊及傳輸系統，並重視隱私議題。此外，非必要性地限制或增加資訊流動規定，也會對全球性的商業經濟活動造成負面影響。因此，有必要發展一套可保護個資與兼顧全球經濟發展活動的隱私制度，促進 APEC 會員經濟體之個資蒐集、存取、利用或處理的組織發展，並執行有關個資存取與利用的全球化標準程序，因而制定 APEC 隱私保護綱領，其內容與 OECD 1980「隱私保護與個人資料之國際傳遞指導方針」的核心價值相符，包括 9 項 APEC 隱私保護原則，並舉例說明實務面相關作法。

(1)預防損害(Preventing Harm)

包括指派組織內負責個資管理之專責人員角色、建立適當之管理機制，以及當發生個資事故時之即時通知與處理措施等。

(2)告知(Notice)

符合法令要求與個資當事人需求之告知程序與形式，包括告知之時機、方式、應涵蓋的內容、確認方式及例外處理原則等。

(3)蒐集限制(Collection Limitations)

明確定義個資類別與其相關之蒐集限制條件、進行蒐集之依據、當事人同意之方式及有效期限之設定等。

(4)個人資料之利用(Uses of Personal Information)

須符合蒐集目的與範圍內之利用，明確定義例外處理原則等。

(5)當事人自主(Choice)

當事人對其個資進行查詢、閱覽、製給複製本、補充或更正、要求停止蒐集、處理或利用及刪除等權利須予以保障，並在適當時限內回應等。

(6)個人資料之完整性(Integrity of Personal Information)

依據當事人自主或蒐集時限屆滿等需求，即時維護個資之完整性與保存狀態等。

(7)安全管理(Security Safeguards)

採行適當之安全措施，以防止個資遭受到竊取、竄改、毀損、遺失或洩漏等情況。

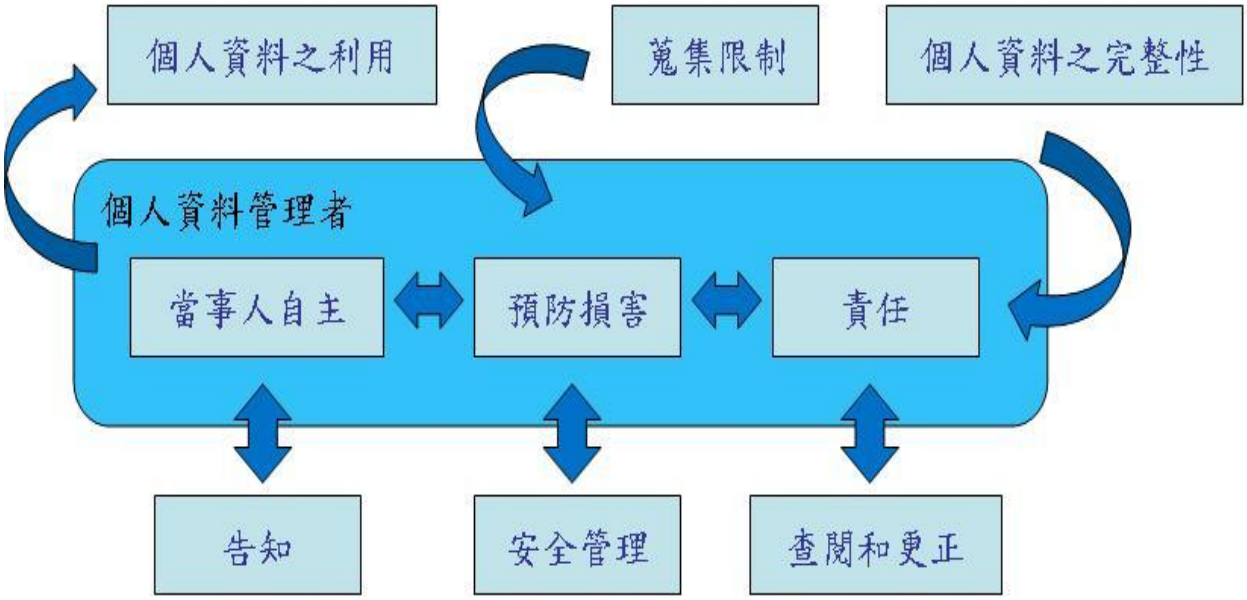
(8)查閱和更正(Access and Correction)

依據當事人自主對於個資查閱或更正之需求適時回應，此外須公告所蒐集個資之檔案名稱、蒐集組織與聯絡人資訊、保有之依據及特定目的、個資類別等資訊，以提供公眾進行查閱等。

(9)責任(Accountability)

規範當個資進行傳輸時，相關處理組織與人員之角色與責任，以避免個資之不當運用，同時保障當事人之隱私權等。

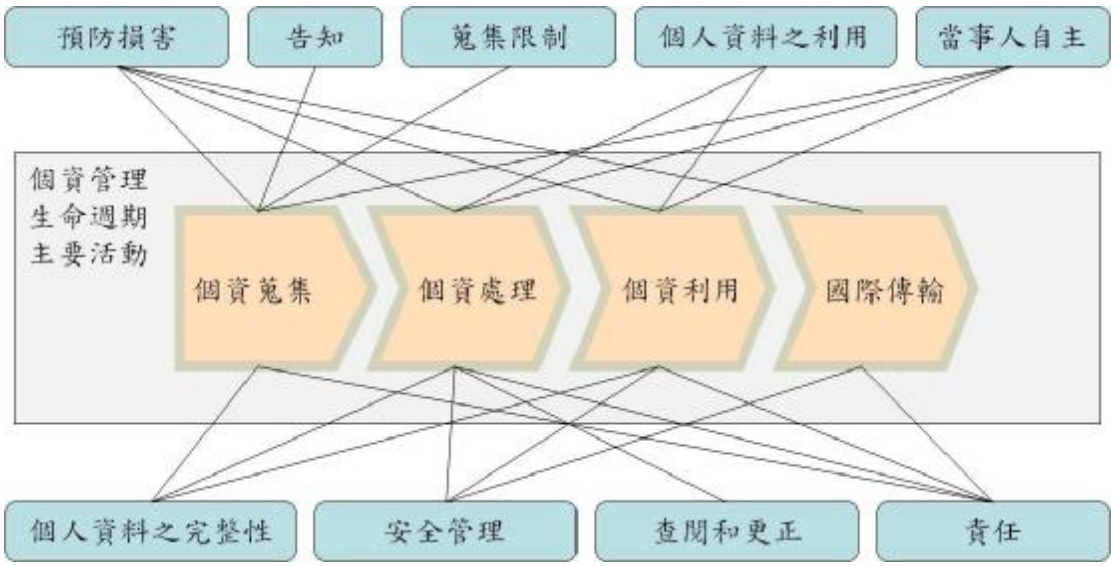
上述 9 項 APEC 隱私保護原則與個人資料管理者間之關聯性，詳見圖 1。



資料來源： 本計畫整理

圖1　APEC 隱私保護原則關聯圖

APEC 隱私保護原則與個資法之個資管理生命週期主要活動之關聯性，詳見圖 2。



資料來源： 本計畫整理

圖2　APEC 隱私保護原則與個資法內容之關聯性

2.2.2. OECD 隱私保護及個人資料之國際傳輸指導方針

經濟合作發展組織(Organization for Economic Co-operation and Development, OECD)於 1980 年發布之「隱私保護及個人資料之國際傳輸指導方針(Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data) 」，已成為國際組織(如 APEC 等)與國家制定其相關隱私保護綱領、原則之參考。OECD 隱私保護及個人資料之國際傳輸指導方針明列 8 大原則如下：

(1)限制蒐集原則(Collection Limitation Principle)：例如僅蒐集執行活動所需之最小範圍內容之個資，明確列出限制蒐集之個資類別或內容等。

(2)資料品質原則(Data Quality Principle)：例如所蒐集之個資必須明確與蒐集目的有關，且應保持個資內容之正確性與完整性，當個資內容有異動時即時進行更新。

(3)目的明確化原則(Purpose Specification Principle)：例如採用正面表列的方式明確說明對個資進行蒐集之目的，而非概括性用語或類似「...等用途」的說明方式。

(4)限制利用原則(Use Limitation Principle)：例如對於個資之處理、利用及國際傳輸等活動，明確設定程序管控，不逾越特定蒐集目的以外之利用。

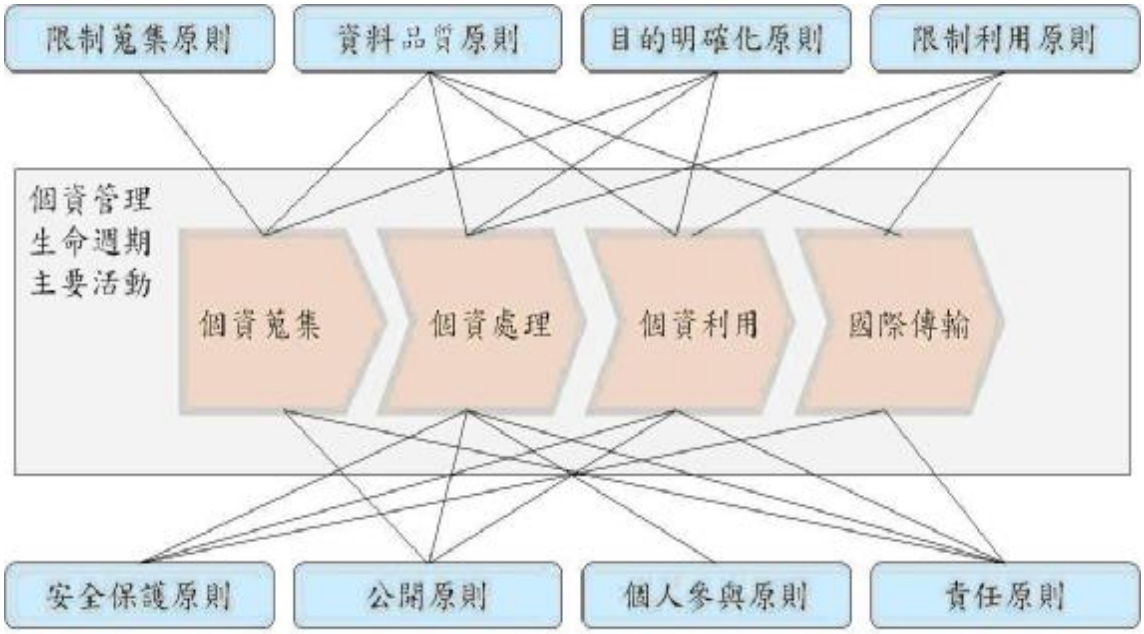
(5)安全保護原則(Security Safeguards Principle)：例如對於個資之處理、利用及國際傳輸等活動中所潛在的揭露風險，建立合適的安全控制措施，如對個資檔案進行加密、設定存取權限及防火牆保護等。

(6)公開原則(Openness Principle)：例如組織主動對外公開所擁有之個資檔案名稱、法律依據、特定目的、保存期間及聯絡窗口等資訊。

(7)個人參與原則(Individual Participation Principle)：例如當事人對於個資自主權之行使像是查閱、更正及要求刪除個資內容等之規範。

(8)責任原則(Accountability Principle)：例如建立個資管理組織人員之職責職掌，使相關人員能夠依循相關政策與程序進行個資管理活動。

有關 OECD 隱私保護指導方針與個資管理生命週期主要活動之關聯性，詳見圖 3。



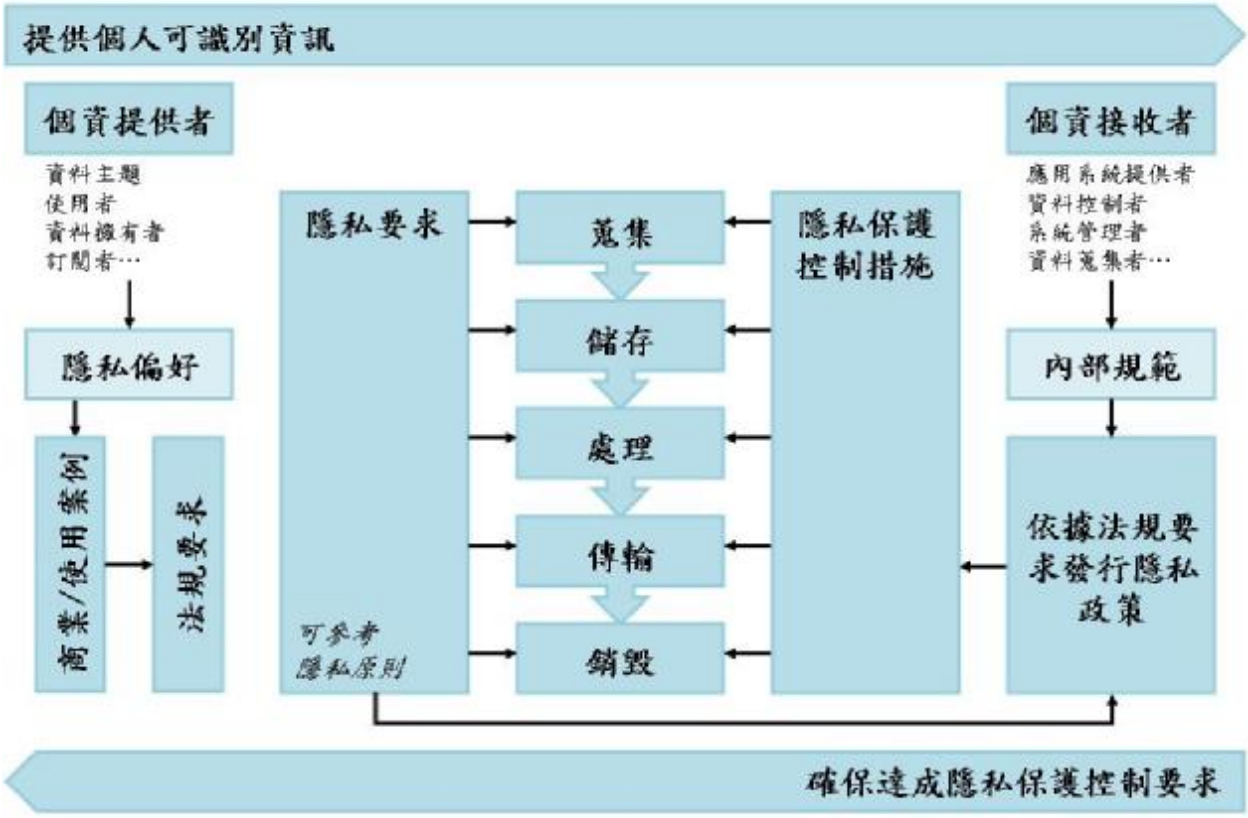
資料來源： 本計畫整理

圖3 OECD 隱私保護指導方針與個資法內容之關聯性

2.2.3. ISO/IEC 29100 資訊科技-安全技術-隱私框架(Information technology-Security techniques-Privacy framework)

2.2.3.1. 內容概述

- 公布日期: 2011 年 12 月 15 日。
- 規劃個資提供者與接收者之間，有關個資蒐集、儲存、處理、傳輸及銷毀等作業流程內容，詳見圖 4。



資料來源： Rannenberg, K. (WG5 Convener), Sténuit, C. (Co-editor 24760), Yamada, A. (Editor 24761), and A.S. Weiss (Editor 29100/29101) (2007) Working Group 5 Identity Management and Privacy Technologies Within ISO/IEC JTC 1/SC 27-IT Security Techniques (Presentation), 2007-09-30，本報告中文化翻譯

圖4　ISO/IEC 29100 隱私框架示意圖

2.2.4. ISO 22307 金融服務-隱私衝擊分析(ISO 22307 Financial services-Privacy impact assessment)

2.2.4.1. 內容概述

- 公布日期: 2008 年 5 月 1 日。
- 由於電腦與網路的快速發展，促進金融服務組織能夠比以往更快速地記錄、保存及處理大量的當事人資料，同時也帶來對於個人隱私權侵犯的

衝擊影響。而金融服務組織在運用當事人個資時，除了考量法規命令的要求外，亦要評估相關金融系統在開發與更新時，是否有妥善保護與避免不當使用當事人的資料，以提升對當事人的作業流程與服務。

- 為確保符合 OECD 隱私原則，組織應建立適當的隱私政策與實作方式，透過標準化的隱私衝擊評估活動，協助組織識別與隱私有關的風險，包括如何降低這些風險，協助組織建立隱私政策與實作方法。
- 由於隱私保護的要求在不同國家有所不同，此標準化的隱私衝擊評估工具，特別適用於含有跨境金融交易的全球性銀行。

2.2.4.2. 範圍

- 提供一個適用於金融服務組織與其委外廠商的隱私衝擊分析(PIA)標準工具，以進行 ISO 22307 隱私衝擊評估流程時之 6 大項目內容，詳見圖 5。
- 說明一般進行隱私衝擊分析評估時的相關活動。
- 定義進行隱私衝擊評估時，所需要之項目內容。
- 做為使用者學習隱私衝擊評估時之相關資訊指引。

資料來源： 本計畫整理

圖5　ISO 22307 隱私衝擊評估流程 6 大項目

2.2.4.3. 目的

- 確保當開始進行一個規劃中的金融系統與相關後續活動時,隱私保護永遠是整個系統發展生命週期中被列為核心考量的課題。
- 確保隱私議題之責任，清楚定義與結合系統開發者、管理者、相關組織及有管轄權人員之工作職責。
- 提供決策者針對規劃中的金融系統，基於隱私與風險間的關聯，決定適當的告知政策、系統設計及購置等，以避免或降低可能之風險。
- 降低當金融系統建置之後，如需終止或持續修改時的風險，以符合隱私的要求。
- 提供作業流程與個資流程的文件，協助組織內部人員用於回應當事人、隱私主管機關或利害關係人對於相關議題之諮詢。

2.2.4.4. 金融機構隱私衝擊分析主要涵蓋領域

- 起始隱私告知：包括評估在應用系統需求分析、設計、開發、測試及上線運作各階段活動中，對於隱私保護之措施與作法是否適當。
- 年度隱私告知：對當事人定期性告知最新隱私政策內容。
- 隱私告知之內容：例如蒐集組織名稱、目的、蒐集之內容及將被使用之方式等。
- 退出(opt-out)/選定(opt-in)政策與告知：例如透過明顯標示提醒當事人可方便自主選擇對隱私之蒐集、處理及利用等方式是否接受或拒絕。
- 變更告知：例如當所蒐集之個資或隱私內容之處理、利用目的或方式，和原本蒐集目的已有變更不同時，是否能即時告知當事人並取得同意。
- 傳遞方式：評估應用系統在傳遞個資檔案時，是否已建立適合的保護機制，例如加密的傳輸管道、權限及密碼控管等。
- 揭露至非分支機構的第三方之限制：例如在蒐集目的告知時，即正面表列出參與之相關第三方，以及相關之執行方式與範圍等。
- 再揭露與再使用資料之限制：例如對於是否即時告知當事人並取得同意後方可進行之管控措施。
- 服務提供者與聯合行銷的退出(opt-out)/選定(opt-in)之例外要求。
- 處理與服務交易的退出(opt-out)/選定(opt-in)與告知之例外要求。
- 退出(opt-out)/選定(opt-in)與告知之其他例外要求。

2.2.5. BS 10012 資料保護-個資管理系統規格(BS 10012:2009 Data protection-Specification for a Personal Information Management System)

2.2.5.1. 內容概述

- 公布日期：2009 年 5 月。

- 目的：提供一個保持與提升符合資料保護之法規與良好實踐之架構。
- 應用「Plan」、「Do」、「Check」及「Act」循環，持續提升管理系統維運要求。
- 主要依循英國資料保護法(The DPA-The Data Protection Act 1998)，DPA 係依據歐洲經濟區(European Economic Area, EEA)的 European Directive(95/46/EC)所制定。個資在 DPA 稱為 Personal Data，BS 10012 則以 Personal Information 代表。
- DPA 由英國資訊專員辦公室(Information Commissioner)負責資料保護相關規劃、管理、教育及監督等事宜。

2.2.5.2. BS 10012:2009 中 8 項資料保護原則

- 公平與合法的處理：例如依據個資法之規範進行個資管理。
- 僅獲取符合符定目的的資料，並於後續處理資料時不逾越這些目的。
- 適當、相關、不過度：應用限制蒐集原則、僅蒐集所需最少的個資。
- 正確與更新：提供當事人自主權利行使時的管道和便利的方式。
- 不保留超出所需的時間：明確定義相關個資檔案之保存期限，和到達期限後之處理方式。
- 處理程序符合法律賦予個人的權利，包括有關存取的權利。
- 保持安全。
- 未經適當的保護措施不得傳輸至 EEA 以外的國家。

2.2.5.3. BS 10012:2009 標準架構

- 簡介(Introduction)：說明個資管理系統(Personal Information Management System, PIMS)係提供維護與改善的框架(framework)，以符合個資保護相關法律與實務要求。
- 範圍(Scope)：說明本標準係提供一個共通基礎以管理個人資料，故適用於各種型態的組織。
- 名詞定義與縮寫(Terms, definitions and abbreviations)：定義標準中所提及之各項名詞與縮寫，例如稽核(audit)、程序(procedure)等。
- 規劃 PIMS(Planning for a personal information management system)：說明規劃階段包括的活動項目，本階段的目的為提供 PIMS 實施的方向與支援，以符合個資保護與實務的要求。
- 建置與運作 PIMS(Implementing and operating the PIMS)：說明建置與運作階段包括的活動項目，本階段的目的在於確保組織依照政策中的要求，指派適當的權責人員。
- 監督與檢視 PIMS (Monitoring and reviewing the PIMS)：說明監督與檢視階段包括的活動項目，本階段的目的為確保 PIMS 的效率與有效性受到適時的監督與檢視。
- 改善 PIMS(Improving the PIMS)：說明改善階段包括的活動項目，本階段的目的是藉由矯正行動的實施以改善 PIMS 的效率與有效性。

2.2.5.4. 規劃 PIMS 階段

本階段主要活動包括：

- 定義組織中 PIMS 的範圍與目的：例如建立個人資料保護要點。
- 建立個資管理政策：政策應聲明適用範圍，例如全組織或部分單位。
- 指派適當人員角色職責：例如指派一至多位專業人員負責平時的運作。

- 提供足夠的資源：組織在建置、實施、運作及維護 PIMS 過程中，應提供所需的資源。
- 將 PIMS 與組織文化契合：例如與組織現有的管理制度、程序進行整合運作，降低對人員日常作業的衝擊影響。

2.2.5.5. 建置與運作 PIMS 階段

本階段主要活動包括：

- 指派負責人員：確保組織依據其個資管理政策，指派適當的負責人員。
- 識別與記錄個資的用途：個資之識別可從業務流程或服務目錄著手，主要辨別個資對於流程與活動利害關係人的風險，分析個資的類別，在其不同生命週期的型態、相關文件、支援系統及彼此間的介面，做為後續風險評鑑的重要輸入來源。
- 教育與認知：確保所有人員能夠認知其在處理個資時的職責。
- 風險評鑑：確保組織認知當在處理特定類型的個資時之相關風險。
- 其他 PIMS 日常運作活動：包括公平與合法的處理個資、告知流程、維持 PIMS 為最新狀態、當事人權利、個資保留與銷毀、委外處理流程、對第三方揭露、安全議題及資料正確性等資料。

2.2.5.6. 監督與檢視 PIMS 階段

本階段主要活動包括：

- 內部稽核：例如稽核規劃、稽核員選擇及稽核要求等。
- 管理審查：審查項目應來自個資管理系統使用者之回饋意見、人員所發現並呈報之風險、稽核結果、程序審查紀錄、技術升級或更換的結果、主管機關的正式評鑑要求、抱怨處理及已發生的違反安全事故等。

2.2.5.7. 改善 PIMS 階段

本階段主要活動包括：

- 預防措施與矯正行動：所有變更或改善的建議，應於實施前進行評估，以符合政策上的要求。
- 持續改善活動：透過稽核結果、矯正預防措施及定期檢視的作法，以持續改善 PIMS 的有效性。

2.2.6. NIST SP800-122

2.2.6.1. 內容概述

- 文件名稱：個人可識別資訊機密性保護指引(GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION)
- 公布日期：2010 年 4 月。
- 目的：過去幾年來，包括數百萬筆個資紀錄遺失的資安事故層出不窮，因而對個人與組織造成傷害，如身分竊取、詐騙、信任感喪失、法律責任及矯正成本等。因此，保護個資的機密性實有其必要性，故美國國家標準與技術局(National Institute of Standards and Technology, NIST)制定本文件，主要提供聯邦政府機關及其相關委外單位，於執行個資保護時之參考建議，其他組織亦可參照運用。
- 目標：本文件除說明個資防護的重要性外，並以風險為基礎，建議各項防護措施與事故回應計畫(Incident Response Plan)。
- 文件架構：本文件共分為 5 個章節，第 1 章介紹文件的目的與範圍、使用對象及文件架構；第 2 章描述何謂個資，並如何找出組織所維護的個資；第 3 章說明當個資遭到不當的存取、使用及揭露時，如何決定衝擊

等級因素；第 4 章提供保護個資機密性的控制措施，以降低個資被洩漏的風險；第 5 章提出如何發展個資事故回應計畫，並整合至組織現有的事故回應計畫中。

2.2.6.2. 個資辨識

本文件使用廣義的個資定義，以儘可能辨識出個資的可能來源(如資料庫、網路磁碟機分享、備份磁帶及承包商等)。所謂個資係機關所維護的個人任何資訊，包括用來區隔或追蹤個人身分的資訊，例如姓名、社會安全號碼、出生日期與地點、生物特徵(biometric)紀錄等；任何已連結或可連結到個人的資訊，如醫療、教育、金融及雇用資訊。有關個資相關範例如下，但不受此限。

- 姓名，例如全名、別名等。
- 個人身分號碼，例如社會安全號碼、護照號碼、駕照號碼、納稅人身分號碼、金融帳號及信用卡號等。
- 地址資訊，例如住家地址、電子郵件地址等。
- 個人特徵，例如影像、指紋、筆跡或其他生物特徵資料(如視網膜、聲音)等。
- 已連結或可連結至以上範例的資訊，例如種族(Race)、宗教及體重等。

2.2.6.3. 個資運用

當進行個資蒐集、使用及保留時，應限制以完成工作所需的個資項目為主，並儘可能減至所需之最小程度。一旦遭遇個資外洩事故，才能將傷害降到最低。另外，組織應定期檢視以往蒐集的個資以決定是否仍為組織業務所需，如組織可以制訂每年固定一天為個資清除認知日(purging awareness day)。

美國管理預算局(Office of Management and Budget,OMB)於編號為 M-07-16 的備忘錄中，具體提出聯邦政府機關需遵守下列事項。

- 檢視持有之個資，確保其內容是否正確、即時、適當及完整。
- 機關運作過程中，於對個資最小需求的原則下，降低持有之個資數量。
- 定期檢視所持有之個資。
- 針對社會安全號碼不必要的蒐集，建立一個刪除計畫。

2.2.6.4. 個資分類

個資應以衝擊等級(Impact Level)結果去評估其機密性，如此才可以套用適當的保護措施。個資機密衝擊等級可分為低、中、高三種等級，分別表示當個資遭到不當的存取、使用及揭露時，對組織或個人的潛在損害程度。本文件將列出組織於考量機密衝擊等級時之因素，以利組織擬定適當的政策(Policy)、程序(Procedure)及控制措施(Control)。以下是考慮因素的範例，但不受此限。

- 可識別能力(Identifiability)：組織應評估個資是否容易識別出特定的個人。例如，社會安全號碼可唯一且直接識別出個人，而電話區碼則是識別出一群人。
- 個資數量：組織應評估有多少個資數量，25 筆與 2 千 5 百萬筆個資破壞的衝擊是不一樣的。該項因素與機密衝擊等級有密切關係。
- 資料欄位的敏感程度(Data Field Sensitivity)：組織應評估個資欄位的敏感程度，例如，社會安全號碼或金融帳號的敏感程度通常勝於個人電話或郵遞區號。
- 使用情境(Context to Use)：組織應評估個資的使用目的，個資被蒐集、

儲存、使用、處理、揭露及散播的目的。相同的個資元素(Element)可能會因其使用目的而有不同的機密衝擊等級。例如，假設組織擁有兩組相同個資欄位(包括姓名、地址或電話)的清單，第 1 組清單為訂閱由組織發行一般利益(general-interest)電子報的訂閱者，第 2 組清單為在執法機關的秘密工作人員，很顯然地，第 2 組清單若遭到侵害，對個人或組織的潛在衝擊，將明顯不同於第 1 組清單。

- 保護機密性的義務：組織因法律、規範及其他命令的要求(如隱私法、美國管理預算局發行的指引等)，而有義務去保護個資。例如美國人口統計局(Census Bureau)與美國內地稅務局(Internal Revenue Service , IRS)因受到法規要求，而有義務去保護特定型態的個資。
- 個資存取與存放位置：組織可考量授權存取的性質(Nature)與個資存放位置，例如個資頻繁的由人員與系統存取，或是定期地被傳送到異地(Offsite)，那麼個資的機密性就有較多的機會外洩。

2.2.6.5. 個資保護

並非所有個資都使用同一種方式保護，組織應依個資機密衝擊等級，實施適當的保護措施。某些資訊並不需要機密性保護，例如組織已同意公開或授權公開的資訊(如組織公開的電話簿)。美國國家標準與技術局建議使用操作性(operational)與隱私相關的保護與安全控制措施。

- 建立政策與程序：組織應發展全面性的政策與程序，以保護個資的機密性。
- 實施訓練：人員被授權存取包括個資的系統之前需接受適當訓練，以降低個資被不當存取、使用或揭露的可能性。
- 個資去識別化(De-Identifying)：當有關個人的全部紀錄(Record)不再需要時，組織得以透過移除足以識別個人的相關資訊，加以去識別化，使

留下來的資訊無法識別出特定之個人。

- 使用存取實施(Access Enforcement)：組織可透過存取控制政策與存取實施機制(access enforcement mechanisms)，如存取控制清單，以控制對個資之存取。
- 實施行動裝置存取控制：組織應禁止或嚴格限制使用可攜式或行動裝置存取個資，例如膝上型電腦(Laptop)、行動電話、個人數位助理(PDA)。
- 提供傳輸的機密性：組織應保護個資傳輸的機密性，通常可透過通訊協定加密或傳輸前資料加密完成。
- 事件稽核：組織應查核影響個資機密性的事件，例如個資不正當之存取。

2.2.6.6. 個資事故回應計畫

個資破壞將對個人與組織造成傷害，透過有效的個資事故回應計畫發展，可將對個人與組織的傷害降到最低。個資事故回應計畫內容應包括當發生個資事故時，需於何時與如何通知到個人、如何進行通報及是否有改善方案等。

2.2.6.7. 密切協調

保護個資之機密性需有資訊系統、資訊安全、隱私及法律需求等相關知識。由於相關法規命令，通常較為複雜且會隨時間變化，因此，需就教於組織內的法務或隱私部門，以決定相關規定之適用性。此外，一些新的政策通常需要技術安全控制措施來達成，故密切地協調組織內的個資相關專家(如隱私長、資訊長、資安長及法律顧問等)，確保個資安全要求被妥適地施行，以預防個資外洩事故發生。

2.3.我國個資相關規範

「電腦處理個人資料保護法」於 84 年 8 月 11 日公布施行，當初規範非公務機關之適用主體有行業類別之限制，僅限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八行業，一般行業與個人均不受規範，保護之客體亦只限於經電腦處理之個資，不包括非經電腦處理之個資，對於保護個資隱私權益之規範顯有不足，故法務部自 90 年起即積極進行相關修法工作，於整理國內學界與實務界之修法意見，並參酌各國個資保護之立法例，經召開多次公聽會與研討會後，研擬「電腦處理個人資料保護法修正草案」，報請行政院審查，行政院院會業於 93 月 9 月 8 日通過，並函送立法院審議。

法務部所擬電腦處理個人資料保護法修正草案(修正後名稱為「個人資料保護法」)，歷經多年來審查、協商及立法院「屆期不續審」再重報，終於在 99 年 4 月 27 日三讀修正通過，使個資法在保障個人隱私資料，並兼顧新聞自由平衡下邁向新的里程碑，個資法強化個資揭露、查詢及更正等的自主控制，同時也將「亞太經濟合作論壇(APEC)隱私保護綱領」所揭示的預防損害、告知及蒐集限制等 9 項原則納入規範，以迎接個資保護全球化時代的來臨。個資法內容條款與 APEC 資訊隱私保護 9 項原則之間，主要對應關係詳見表 3。

表3　我國個資法條款與 APEC 資訊隱私保護 9 項原則之對應

APEC 資訊隱私保護 9 項原則	個資法條款
預防損害(Preventing Harm)	§12、§18、§27~§40
告知(Notice)	§7~§9
蒐集限制(Collection Limitations)	§6、§15、§19、§53
個人資料之利用(Uses of Personal Information)	§5、§16、§20
當事人自主(Choice)	§3、§10、§11、§13
個人資料之完整性(Integrity of Personal Information)	§11
安全管理(Security Safeguards)	§27
查閱和更正(Access and Correction)	§3、§10~§11、§13、§17
責任(Accountability)	§21

資料來源： 本計畫整理

2.3.1. 個資法修正重點

- 擴大保護客體

「電腦處理個人資料保護法」保護對象只限於經電腦處理之個資，非經電腦處理之個資，則不在該法適用範圍內，造成保護漏洞，有失平衡，且各國立法例亦均將其列入保護客體。因此，為落實對個資之保護，本次修法將保護客體予以擴大，不再以經電腦處理之個資為限，將人工資料併予納入。另外在保護範圍增列護照號碼、醫療、基因、性生活、健康檢查、前科紀錄及聯絡方式等得以直接或間接識別該個人之資料。

- 普遍適用主體

– 刪除非公務機關行業別之限制，即任何自然人、法人或其他團體，除為單純個人或家庭活動之目的，而蒐集、處理或利用個資外，皆須適用本法。

– 增訂公務機關及非公務機關，在中華民國領域外對中華民國人民蒐集、處理或利用個資者，亦有本法之適用。

– 個資增加護照號碼、醫療、基因、性生活、健康檢查、前科紀錄及聯絡方式等得以直接或間接識別該個人之資料。

Ÿ 增修行為規範

– 增訂有關醫療、基因、性生活、健康檢查及犯罪前科等資料為特種個資，其蒐集、處理或利用之要件較一般個資更為嚴格。特種個資原則上不得蒐集、處理或利用，須符合法定要件始得為之。

– 增訂本法所稱之書面同意，須經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。如係特定目的外利用個人資料需當事人書面同意者，不得以概括方式取得其同意，而應另以單獨書面同意方式為之，以確保當事人之權益。

– 增訂蒐集資料時不論是直接或間接蒐集，除符合得免告知情形者外，均須明確告知當事人蒐集者名稱、蒐集目的、資料類別、利用方式及資料來源等相關事項。

– 對於違反本法規定所蒐集、處理或利用之個人資料，增訂公務機關應主動或依當事人之請求，刪除、停止蒐集、處理或利用其個人資料；蒐集機關所保有之個人資料檔案，因未為更正或補充致造成不正確者，如係可歸責於該蒐集機關之事由，應於更正或補充後，通知曾提供利用之對象，使該資料能即時更新，避免當事人權益受損。

– 為尊重個人生活，減少不必要之干擾，對於不論是特定目的內或特定目

的外之行銷行為，增訂該從事商品行銷之非公務機關，應於首次行銷時免費提供當事人表示拒絕之方式；當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷，以尊重當事人有拒絕接受行銷之權利。

Ÿ 強化行政監督

為加強防制個人資料之濫用，中央目的事業主管機關或直轄市、縣(市)政府，發現非公務機關違反本法規定或認有必要時，得派員攜帶執行職務證明文件，進入檢查，如發現有違法情事，並得採取必要處分。

Ÿ 促進民眾參與

– 增訂財團法人或公益社團法人符合本法規定者，得代受害之當事人提起團體訴訟，以協助其救濟遭侵害之隱私權益。

– 為鼓勵民眾樂於利用公益團體機制，提起團體訴訟保護自己之權利，增訂財團法人或公益社團法人接受被害當事人 20 人以上訴訟實施權之授與後，得以自己名義提起損害賠償訴訟。

2.3.2. 對政府機關之衝擊

面對個資法之施行，政府機關即將面對的主要衝擊如下：

Ÿ 保護客體範圍擴大

新法不僅限於舊法所規範的電腦處理個資，包括直接、間接識別之個資或人工資料(書面文件)。

Ÿ 作業流程調整需求

在個資流程生命週期內各階段活動，包括主動告知與取得同意義務的實踐與責任、當事人權利行使時之回應與處理、委外作業權責定義與合約監督管理、個資事故流程之管理與檢討等。

Ÿ 舉證與處罰之預防

應更主動建立隱私保護政策與規範、定義適當個資管理組織人員權責、提升安全控制措施至合適等級、保存重要個資管理與數位鑑識紀錄，以及持續進行人員認知與訓練等。

2.3.3. 政府機關應注意事項

個資法對政府機關處理人員而言，須特別注意之規範內容如下：

Ÿ 蒐集與處理：第十五條，公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

– 執行法定職務必要範圍內。

– 經當事人書面同意。

– 對當事人權益無侵害。

Ÿ 個資直接蒐集之免告知情形：依據個資法第八條，下列情形得免告知，直接向當事人進行資料蒐集：

– 依法律規定得免告知。

– 個人資料之蒐集係公務機關執行法定職務。

– 告知將妨害公務機關執行法定職務。

– 告知將妨害第三人之重大利益。

– 當事人明知應告知之內容。

Ÿ 間接個資蒐集之告知事項：依據個資法第八條，除前項情形外，公務機關直接向當事人蒐集資料時，應告知當事人：

– 公務機關名稱。

– 蒐集之目的。

– 個人資料之類別。

– 個人資料利用之期間、地區及對象及方式。

– 當事人依第三條規定得行使之權利及方式。

– 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。

Ÿ 利用：第十六條，公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

– 法律明文規定。

– 為維護國家安全或增進公共利益。

– 為免除當事人之生命、身體、自由或財產上之危險。

– 為防止他人權益之重大危害。

– 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後，或蒐集者依其揭露方式無從識別特定之當事人。

– 有利於當事人權益。

– 經當事人書面同意。

Ÿ 公開事項：第十七條，公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

– 個人資料檔案名稱。

– 保有機關名稱及聯絡方式。

– 個人資料檔案保有之依據及特定目的。

– 個人資料之類別。

Ÿ 專人專責與損害賠償：第十八條，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。第二十八條，公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

2.3.4. 政府機關應立即研辦事項

有關各目的事業主管機關其應辦理之事項(例如相關施行細則等)，已由法務部進行中。同時依據行政院函，各公務機關在個資法施行前，應立即研辦事項主要包括：

Ÿ 公開下列事項於電腦網站上，提供公眾查閱：

– 個人資料檔案名稱。

– 保有機關名稱及聯絡方式。

– 個人資料檔案保有之依據及特定目的。

– 個人資料之類別。

Ÿ 指定專人辦理個人資料檔案安全維護事項。

2.3.5. 正式施行期程

依據個資法第五十六條本法施行日期，由行政院定之。其施行日期經法務部於 101 年 9 月 26 日完成施行細則修訂頒布後，由行政院頒布本法除第 6 條、第 54 條外施行日期為 101 年 10 月 1 日。

有關個人資料保護法施行細則修正要點，摘要說明如下：

- 為明確以間接方式識別該個人資料之意義及提供不能識別該個人資料之判斷標準；醫療、基因、性生活、健康檢查及犯罪前科之概念；刪除、內部傳送、當事人自行公開、已合法公開之個人資料、資料經過處理後或依其揭露方式無從識別特定當事人等概念，增列相關定義性規定，以資衡平個人資料保護與個人資料合理利用。
- 為保護個人資料之隱私權，個人資料檔案除了備份檔案之外，亦應包括軌跡資料在內。
- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依個資法第四條規定，於個資法適用範圍內視同委託機關，係指以委託機關為權責歸屬機關，增訂委託人之適當監督義務規定。
- 增訂本法所稱適當安全維護措施、安全維護事項或適當之安全措施之事項內容規定。
- 增訂個資法所稱書面意思表示之方式及單獨所為之書面意思表示之意涵。
- 增訂個資法規定告知之方式。

此外，施行細則第 12 條所述之必要措施，共計 11 項：

- 配置管理之人員及相當資源：專人、專責組織負責個資保護相關事宜。
- 界定個人資料之範圍：即進行個資盤點，必須知道誰使用那些資料並且存放在什麼位置，包括紙本和電子個資。
- 個人資料之風險評估及管理機制：應針對個人資料進行風險評估，並提供相關管理機制。
- 事故之預防、通報及應變機制：規範個資事故發生後的通報應變流程。
- 個人資料蒐集、處理及利用之內部管理程序：制定個資保護相關的執行

程序與標準作業流程。

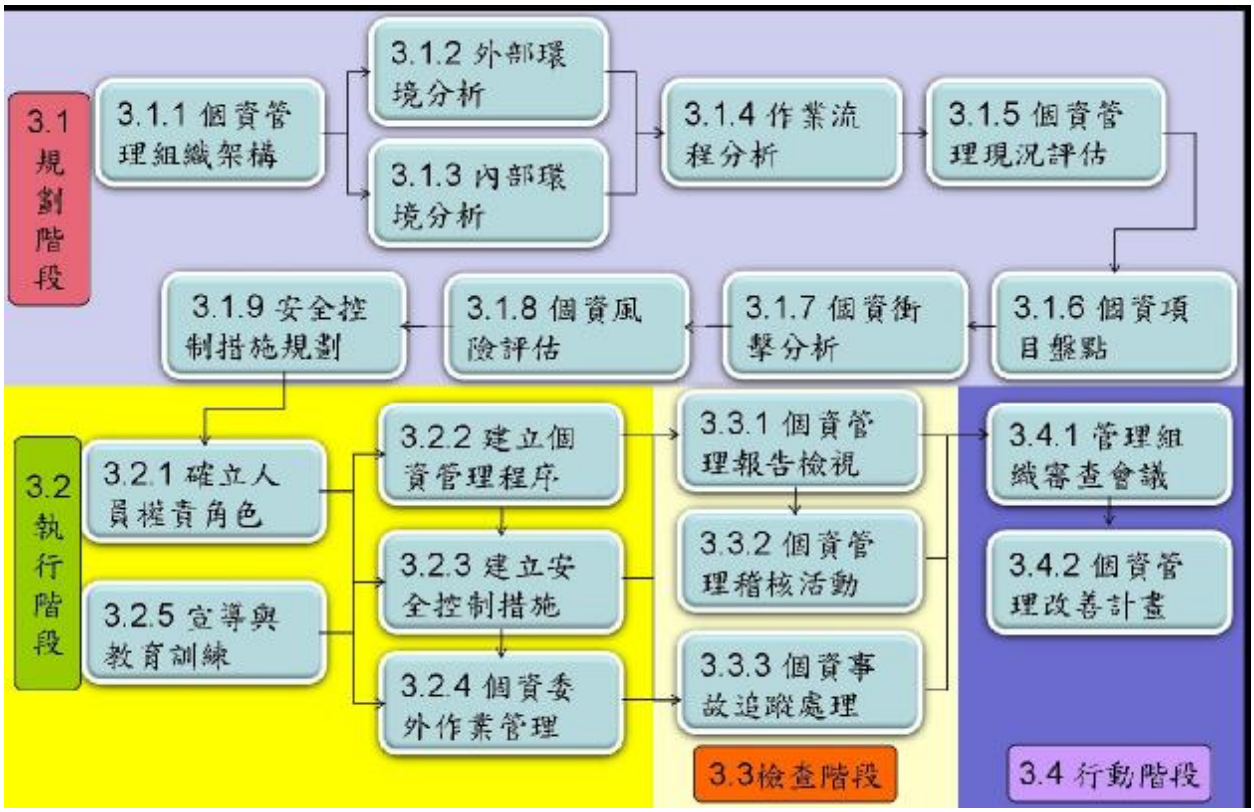
- 資料安全管理及人員管理：說明對個資應該採取何種 IT 科技與系統進行保護；人員存取個資的權限管制等。
- 認知宣導及教育訓練：對於同仁應施行適當的個資宣導與訓練。
- 設備安全管理：針對各種保存個資的載具或系統，應定期的維護與更新。
- 資料安全稽核機制：對於存放個資的 IT 系統定期進行資料稽核。
- 使用紀錄、軌跡資料及證據之保存：IT 設備或者紙本資料個資存取控制的紀錄、日誌檔（Log）等，都必須完整保留，這些都可能是舉證的證據力。
- 個人資料安全維護之整體持續改善：針對個資保護不足之處持續更新。

3. 個資保護管理建置流程

個資保護管理建置流程之目的，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，遵循國際標準管理系統的 PDCA 循環分為規劃、執行、檢查及行動 4 個階段，每個階段分別有不同的活動(Activity)，例如個資管理組織架構、個資項目盤點、個資衝擊分析、個資風險評估、建立個資管理程序及建立安全控制措施等。其中每項活動中有不同的任務(Task)需要執行，而過程中可能需要各種不同資訊的提供，再輔以各種執行手法與相關工具，完成該項任務，任務如有產出將可能成為其他任務或活動執行時所需參考之資訊。例如在「個資管理組織架構」活動中，需要進行「瞭解組織現行架構(含單位別與功能性)和人員角色職責」之任務，因此，必須先瞭解「單位組織圖、管理制度架構圖、角色職責分工定義」等資訊，並透過「資料蒐集、人員訪談」方式，達成該項任務之目的，最後再進一步去定義「個資管理組織」架構。

個資保護管理建置流程之整體發展架構，詳見圖 6，有關各階段之活動分述如下：



資料來源： 本計畫整理

圖6 個資保護管理建置流程之整體發展架構

Ÿ 規劃階段

– 活動：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，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。

– 活動：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。

– 活動：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。

– 活動：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。

– 活動：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。

– 活動：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。

– 活動：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行動方案，避免個資洩露事故之發生。

– 活動：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。

– 活動：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。

Ÿ 執行階段

– 活動：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。

– 活動：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。

– 活動：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。

– 活動：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。

– 活動：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。

Ÿ 檢查階段

– 活動：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，適時提出矯正預防行動方案，以持續提升組織個資管理成效。

– 活動：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。

– 活動：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。

Ÿ 行動階段

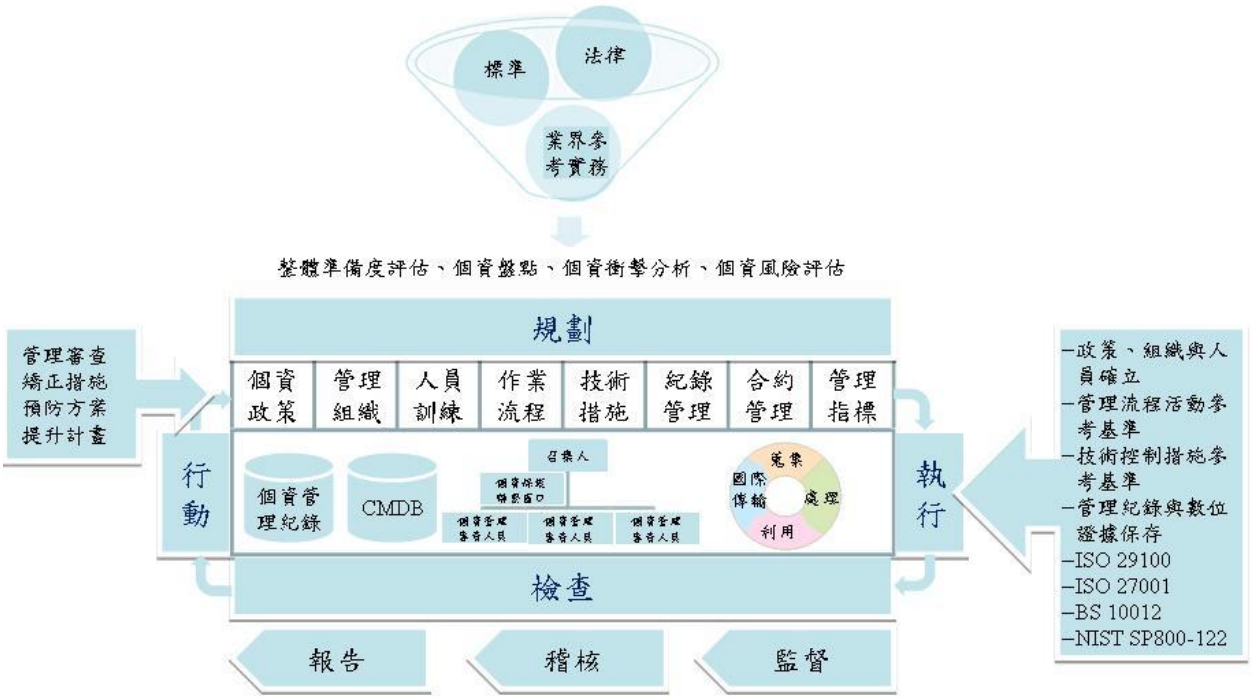
– 活動：管理組織審查會議

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。

– 活動：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，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。

個資管理對任何組織而言，需要隨時因應組織內外部發展趨勢、法律、規範及環境的變化，進行調整與持續提升改善。因此，組織可運用規劃(Plan) 、執行(Do)、檢查(Check)及行動(Act)的 PDCA 循環作業，持續進行改善，詳見圖 7。



資料來源： 本計畫整理

圖7 個資保護管理建置流程 PDCA 持續改善循環

此外，由於政府推動資訊安全管理系統(Information Security Management

System, ISMS)政策已多年，對於已通過 CNS/ISO/IEC 27001 驗證或建立 ISMS 制度的機關而言，如何以既有資訊安全管理制度為基礎，加強個資保護管理需求，亦是一個重要課題。因此，針對已實施資訊安全管理系統，建議加強之個資管理需求，將於 3.5 節中說明。以下依據個資保護管理建置流程，分別說明各階段之活動項目、任務內容。

3.1.規劃

規劃階段主要先針對組織內個資管理現況、內外環境的個資需求及組織作業流程中可能與個資相關項目，進行整體瞭解，並架構出個資管理所需之功能性組織，再整合前項個資管理整體準備度與主要風險領域評估的結果、個資盤點整理出之個資流程與項目及應用系統個資衝擊分析結果等，進行個資衝擊分析與個資風險評估，藉此瞭解組織所蒐集、處理及利用相關個資之風險等級，並對應至適當的安全控制項目基準值，做為發展技術控制措施，後續個資管理與防護實作的依據。

本階段之活動包括個資管理組織架構、外部環境分析、內部環境分析、作業流程分析、個資管理現況評估、個資項目盤點、個資衝擊分析、個資風險評估及安全控制措施規劃，有關本階段之輸入項目、產出項目、執行方法與相關工具及任務分工，詳見表 4，分述如下：

表4　規劃階段活動與任務表

活動與任務 (Activity & Task)	輸入項目 (Input)	產出項目 (Output)	執行方法與相關工具 (Technique & Tool)
Activity1：個資管理組織架構			
Task1：瞭解組織現行架構(含單位別與功能性)與人員角色職責	單位組織圖、管理制度架構圖、角色職責分工定義		資料蒐集、人員訪談
Task2：定義個資管理組織		個資管理組織架構圖	人員訪談、個資管理組織與角色職責分工範例
Task3:定義個資管理組織人員角色職責		個資管理組織角色職責定義	個資管理組織與角色職責分工範例
Task4：建立個資管理政策與要點		個人資料保護管理要點	個人資料保護管理要點範例
Task5：發布個資管理組織架構		個資管理組織架構圖	內部公告、電子郵件、網站
Activity2：外部環境分析			
Task1：瞭解個資管理相關法令、規範、準則等之遵循需求	個資法與相關施行細則、行政命令、準則	個資管理應完成事項清單	資料蒐集與分析
Task2：瞭解個資管理相關國際標準、原則等之遵循需求	個資管理相關國際標準、原則	個資管理應完成事項清單	資料蒐集與分析
Task3：外部利害關係人分析	外部利害關係人	個資有關之利害關係人清單	資料蒐集與分析、人員訪談、個資項目盤點表範例
Activity3：內部環境分析			
Task1:瞭解現有管理制度內容與應用範圍	現有管理制度政策與文件		資料蒐集、人員訪談

活動與任務 (Activity & Task)	輸入項目 (Input)	產出項目 (Output)	執行方法與相關工具 (Technique & Tool)
Task2：內部利害關係人分析	內部利害關係人	個資有關之利害關係人清單	資料蒐集與分析、人員訪談、個資項目盤點表範例
Task3：分析個資管理涵蓋範圍	與個資有關之利害關係人清單		資料分析、個資項目盤點表範例
Task4：定義組織個資管理導入各階段範圍		個資管理導入各階段範圍定義	人員訪談
Activity4：作業流程分析			
Task1：分析服務目錄與服務等級協議	服務目錄(Service Catalogue)、服務等級協議(SLA)		資料蒐集、人員訪談
Task2：分析業務作業流程	業務作業管理文件程序與規範		資料分析、人員訪談
Task3：分析委外作業流程	委外作業程序與規範、委外契約(Contract)		資料分析、人員訪談
Task4：定義和個資相關之流程與應用系統範圍		個資有關之作業流程、應用系統清單	個資項目盤點表範例
Activity5：個資管理現況評估			
Task1：進行組織個資管理現況評估	組織個資管理現況資料與紀錄		人員訪談、個資管理整體準備度評估問卷
Task2：分析個資管理現況評估資料	訪談與問卷紀錄		資料分析、人員訪談、個資管理整體準備度評估問卷

活動與任務 (Activity & Task)	輸入項目 (Input)	產出項目 (Output)	執行方法與相關工具 (Technique & Tool)
Task3：產出組織個資管理現況評估分析結果		個資管理現況評估報告	個資管理整體準備度評估問卷
Activity6：個資項目盤點			
Task1：識別不同作業流程之個資項目	個資管理導入各階段範圍有關之作業流程、應用系統清單	個資流程分析表	資料蒐集與分析、人員訪談
Task2：識別個資項目之類別、依據及目的	個資流程分析表	個資項目蒐集範圍、個資項目基本資料表	個資法與相關施行細則、行政命令、準則、資訊系統分類分級與鑑別機制參考手冊
Task3：識別個資項目相關生命週期活動	個資項目基本資料表	個資項目生命週期	資料蒐集與分析、人員訪談、個資項目生命週期範例
Task4：識別個資項目與外部利害關係人之關聯	個資項目基本資料表	個資項目利害關係人	資料蒐集與分析、人員訪談、個資項目利害關係人範例
Task5：完成個資項目盤點	個資項目基本資料表、個資項目生命週期、個資項目利害關係人	個資項目盤點表	資料蒐集與分析、個資項目盤點表範例
Activity7：個資衝擊分析			
Task1：設計個資衝擊分析檢核表		個資項目個資衝擊分析檢核表	資料蒐集與分析、個資衝擊分析檢核表範例
Task2：進行個資項目個資衝擊分析	個資項目盤點表	個資項目個資衝擊分析檢核表	人員訪談、資料蒐集、個資衝擊分析檢核表範例
Task3：完成個資衝擊分析	個資項目個資衝擊分析檢核表	個資項目衝擊分析表	資料分析、個資項目個資衝擊分析檢核表範例、個資項目衝擊分析表範例
Activity8：個資風險評估			

活動與任務 (Activity & Task)	輸入項目 (Input)	產出項目 (Output)	執行方法與相關工具 (Technique & Tool)
Task1：設計個資項目之個資風險等級基準值	個資項目盤點表	個資風險等級基準值建議	資料分析、資訊系統分類分級與鑑別機制參考手冊、個資風險等級基準值建議表
Task2：分析個資項目個資性之風險等級	個資項目衝擊分析表、個資風險等級基準值建議	PIA/RA 安全控制項目基準值	資料分析、資訊系統風險評鑑參考指引
Task3：完成個資風險評估	PIA/RA 安全控制項目基準值	個資項目衝擊評鑑表	資料分析
Activity9：安全控制措施規劃			
Task1：規劃組織安全控制措施	個資保護技術安全控制項目基準值建議、個資項目衝擊評鑑表	組織安全控制措施規劃	研討會、個資保護技術安全控制項目基準值建議表、電子資料保護參考指引
Task2：評估所需資源	組織應處理之衝擊、個資風險等級、個人資料保護管理要點	組織應處理之衝擊	研討會、個資保護技術安全控制項目基準值建議表、電子資料保護參考指引
Task3：確認組織安全控制措施規劃內容	組織安全控制措施規劃	已核可之安全控制措施規劃	個資管理組織架構圖、個資管理組織角色職責定義

資料來源： 本計畫整理

3.1.1. 個資管理組織架構

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。

個資管理組織架構之任務，包括瞭解組織現行架構(含單位別與功能性)與人員角色職責、定義個資管理組織、定義個資管理組織人員角色職責、建立個資管理政策與要點及發布個資管理組織架構。有關每項任務內容，說明如下：

- 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。

- 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。

- 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 5。

表5　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 ▪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

組織架構角色	工作職掌
	▪ 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
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

Ÿ 建立個資管理政策與要點

個資管理政策與要點為組織內對個資管理之最高指導原則，應於核定後公告至所有同仁，並納入一階文件進行維護管理。政策內容包括目的、目標、原則及適用範圍；要點包括個資管理組織架構說明、個資範圍、如何蒐集/處理/利用個資、當事人行使權利之處理及個資檔案安全維護等。有關要點與政策內容建議，詳見附件 2 與附件 3 所示。

Ÿ 發布個資管理組織架構

個資管理組織架構經核定後，應將此組織架構、個資管理政策與要點，透過電子郵件、內部網站或書面文件等方式，公告通知所有同仁。

3.1.2. 外部環境分析

個資保護議題普遍受到國際上的重視，因此，分別提出相關法規、規範或準則，藉以規範持有個資之組織，必須善盡保管的職責。我國亦參考國際個資保護相關資訊，制定個資法與其施行細則，故組織於實施個資保護時，應瞭解個資法與其施行細則之相關要求，並分析持有之個資與那些外部利害關係人有關。

外部環境分析之任務，包括瞭解個資管理相關法規命令之遵循需求，瞭解個資管理相關國際標準與原則之遵循需求，以及分析外部相關利害關係人。有關每項任務內容，說明如下：

Ÿ 瞭解個資管理相關法規命令之遵循需求

針對個資法與其施行細則，瞭解其相關要求，以確保組織於實施個資管理時，能符合法規相關要求。例如個資法第 17 條，公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同。

– 個人資料檔案名稱。

– 保有組織名稱及聯絡方式。

– 個人資料檔案保有之依據及特定目的。

– 個人資料之類別。

故組織於瞭解上述項目之要求後，應確實備齊相關資訊，並置於網站或以其他方式公告。

Ÿ 瞭解個資管理相關國際標準、原則等之遵循需求

由於國際上相當重視個資保護與隱私議題，因此，積極地制定標準、規範或綱領，以確保個資於蒐集、存取、利用或處理期間受到有效保護。組織於建置個資管理制度時，除應遵守個資法之規定外，亦可針對國際上相關標準(詳見 2.2 節)進行瞭解，以強化組織之個資保護安全措施。例如，在 APEC 資訊隱私保護原則中之預防損害(Preventing Harm)原則，組織應指派負責個資管理之專責人員角色、建立適當之管理機制及發生個資事故需即時通知與處理措施等。因此，當組織瞭解法規或國際標準相關要求後，建議可試擬「個資管理應完成事項清單」，做為日後落實個資管理項目之目標。以下即為「個資管理應完成事項清單」範例：

– 配置管理之人員及相當資源：專人、專責組織負責個資保護相關事宜。

– 界定個人資料之範圍：即進行個資盤點，必須知道誰使用那些資料並且存放在什麼位置，包括紙本和電子個資。

– 個人資料之風險評估及管理機制：應針對個人資料進行風險評估，並提供相關管理機制。

– 事故之預防、通報及應變機制：規範個資事故發生後的通報應變流程。

– 個人資料蒐集、處理及利用之內部管理程序：制定個資保護相關的執行程序與標準作業流程。

– 資料安全管理及人員管理：說明對個資應該採取何種 IT 科技與系統進行保護；人員存取個資的權限管制等。

– 認知宣導及教育訓練：對於同仁應施行適當的個資宣導與訓練。

– 設備安全管理：針對各種保存個資的載具或系統，應定期的維護與更新。

– 資料安全稽核機制：對於存放個資的 IT 系統定期進行資料稽核。

– 使用紀錄、軌跡資料及證據之保存：IT 設備或者紙本資料個資存取控制的紀錄、日誌檔（Log）等，都必須完整保留，這些都可能是舉證的證據力。

– 個人資料安全維護之整體持續改善：針對個資保護不足之處持續更新。

Ÿ 外部利害關係人分析

組織所擁有之個資可能會與外部利害關係人有關，因此應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、策略聯盟等，列出個資有關之利害關係人清單，以確實掌握個資項目與個資防護範圍。

3.1.3. 內部環境分析

組織可能已實施相關管理制度，如資訊安全管理(ISMS)、資訊科技服務管理(ITSM)等，其中可能與個資相關，因此，應先瞭解現行管理制度內容與應用範圍，並分析有那些內部利害關係人與個資相關以及個資管理所涵蓋範圍，最後決定個資管理的導入作法。

內部環境分析之任務，包括瞭解現行管理制度內容與應用範圍、內部利害關係人分析、分析個資管理涵蓋範圍及定義組織個資管理導入各階段範圍。有關每項任務內容，說明如下：

Ÿ 瞭解現行管理制度內容與應用範圍

組織在現有實施的管理制度中，部分政策、文件及作法可能與個資相關，為避免資源重複投入，組織應先進行瞭解，後續在建置個資管理時，可以適時地整合在一起。例如個資內稽作業可結合 ISMS 管理制度之稽核活動，共同辦理。

Ÿ 內部利害關係人分析

組織所擁有之個資可能與內部利害關係人有關，因此，應識別與分析和組織間有個資往來活動之內部利害關係人，列出個資有關之利害關係人清單，以確實掌握個資項目與個資防護範圍。此利害關係人清單應與外部利害關係人分析所產生之清單一起彙整。

Ÿ 分析個資管理涵蓋範圍

經由內外環境分析與個資有關之利害關係人清單掌握，組織才能在建置個資管理制度時，決定導入的涵蓋範圍。

Ÿ 定義組織個資管理導入各階段範圍

鑑於組織可能受限於資源(如預算、人員等)限制，必須分階段導入個資管理制度，可定義各階段欲導入範圍。至於導入的優先順序，組織可視法規要求、個資數量等原則決定。例如，行政院於 99/8 /19 函(詳如 2.3.4)請各公務機關在個資法施行前，應立即研辦事項，包括公開個資檔案名稱、聯絡窗口及指定專人辦理個資檔案安全等內容，即可視為優先辦理事項。

3.1.4. 作業流程分析

當組織決定各階段的導入範圍後，接下來應著手分析該範圍內與個資相關流程與應用系統，因此，藉由分析服務目錄、服務等級協議、業務作業流程及委外作業流程的過程，才能準確掌握組織所擁有的個資項目。

作業流程分析之任務，包括分析服務目錄與服務等級協議、分析業務作業流程、分析委外作業流程及定義及個資相關之流程與應用系統範圍。有關每項任務內容，說明如下：

- 分析服務目錄與服務等級協議(Service Level Agreement , SLA)

所謂服務目錄(Service Catalog)係組織提供所有服務項目的列表，這些服務不只是對外的服務，也包括組織內各單位對內部其他單位所提供的服務，例如資訊部門提供之機房維運服務等。另外 SLA 為服務提供者與服務使用者之間的協議，載明使用者要求及提供者承諾，通常 SLA 涵蓋項目包括服務正常運作時間、隱私權、安全及備份程序等。從服務目錄與 SLA 中，發掘可能與個資有關的服務或安全要求，以瞭解目前是否還有不足之處。例如，SLA 中載明針對包括個資的資料應定期進行備份，但卻未定義該備份資料應具有適當的存取控制措施等。

- 分析業務作業流程

就如同導入資訊安全管理制度一樣，從業務作業流程面著手分析，較能夠找出與該業務相關之個資項目，並針對該項目進行適當保護。通常分析業務作業流程，可從與該業務作業管理相關之文件程序與規範著手，例如，人事作業中之招募程序，當對外招募人員時，會收到應徵人員之履歷資料，其中即包括應徵者之個資。

- 分析委外作業流程

對於承接包政府機關委外作業之廠商，如有執行個資蒐集、處理及利用等相關作業時，雖屬非公務機關，但因受公務機關委託，其應遵守之規範與限制，比照公務機關辦理。因此，政府機關於辦理委外作業時，應瞭解該作業是否包括個資項目，除自我要求遵守個資法規定外，更須要求委外廠商亦須遵守個資法。例如，可於契約中要求對委外廠商定期或不定期執行

個資管理稽核作業，以確保廠商落實個資保護相關規定。

Ÿ 定義和個資相關之流程與應用系統範圍

透過服務目錄與流程分析，掌握與個資相關之作業流程與應用系統清單，後續可提供個資項目盤點活動使用。

經由內外部環境分析與作業流程分析的活動產出(如利害關係人清單、服務目錄清單或個資相關應用系統清單等)，可與個資項目盤點表結合。例如，在盤點表中可說明該盤點項目與那些利害關係人相關，那個應用系統會支援該盤點項目並與個資相關，詳見 3.2.1 節。

3.1.5. 個資管理現況評估

組織若欲針對個資管理現況進行評估，可透過個資管理整體準備度評估問卷(詳見附件 4)，進行個資管理整體準備度與主要風險領域評估，藉以了解目前在個資管理較為不足之處與整體個資管理層面上後續應聚焦的重點，做為未來提升與改善之參考。個資管理整體準備度評估問卷係參考 OECD 隱私保護及個人資料之國際傳遞指導方針、APEC 隱私保護綱領等建議之隱私保護構面，針對個資管理各項隱私保護風險領域進行評估，藉由評估結果分析出那些領域是目前個資管理整體準備度較低的部分，相對代表有較高的潛在風險，個資管理整體準備度評估問卷相關風險領域，包括告知/目的、自主/同意、資料蒐集與保存、利用與揭露、正確性、保護/安全性、公開、存取、遵循性與賠償、責任、利益及訓練等。

Ÿ 告知/目的

建立政策及適當管理程序，以證明組織可於合理範圍內保證對於所蒐集之個資，已明確告知當事人其個資被蒐集及使用的目的、範圍及相關管理規範。

Ÿ 自主/同意

協助當事人充分辨別並選擇個資被使用方式(能依個人隱私偏好進行選擇)。

Ÿ 資料蒐集與保存

幫助組織確認並提供合理的保證，所保留之個資與被蒐集的目的相關，且與當事人同意和選擇被利用方式的原則一致，如敏感性個資不應該被保留比必要時間更長。

Ÿ 利用與揭露

協助組織確認當事人資料之公開，於授權的特定對象與限制於特定目的之利用，且與資料被蒐集時，所告知並取得當事人同意的特定目的及其利用範圍是一致的。

Ÿ 正確性

協助組織確認所蒐集個資之正確性且為最新資料，同時無逾越蒐集時所告知之特定目的範圍。

Ÿ 保護/安全性

採取適當量測方式衡量組織對於防止資料外洩、誤用、竄改或破壞等安全維護之強度。有助於確認相關保護措施之有效性，並延伸至第三方委外單位。

Ÿ 公開

建立政策與程序，以確保當事人能夠識別蒐集個資的單位與個資蒐集的特定目的及方式，不逾越特定目的之必要範圍。

Ÿ 存取

確保當事人個資得已被組織合理的處理及利用，且必要時當事人得以要求

更正或修改其個資。

Ÿ 遵循性與賠償

確認組織訂定之政策及程序已遵循個資法及相關法規命令，且建立適當的改善及補強程序(善後執行程序)。

Ÿ 責任

確保組織負有遵循個資法及相關責任。

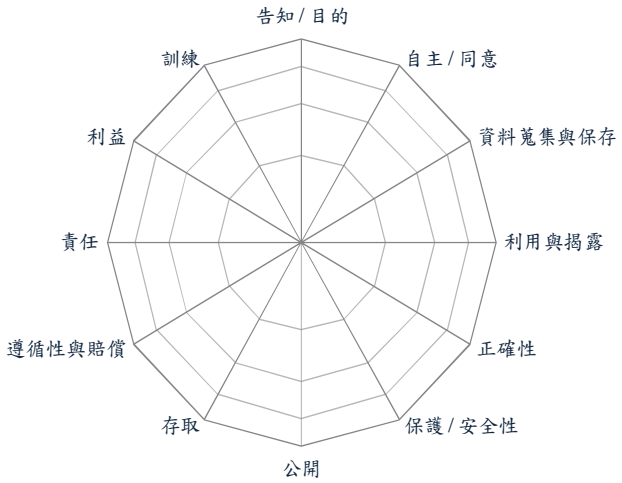
Ÿ 利益

確認組織瞭解良好之個資保護策略與管理框架，將為組織帶來競爭優勢。

Ÿ 訓練

確保組織已訂有適當的個資保護政策及程序之教育訓練。

個資管理整體準備度評估問卷完成後，可利用 Excel 軟體，將各風險領域中符合的比例，繪製成雷達圖，即可瞭解各風險領域的整體準備度情形。針對個資管理整體準備度較低的風險領域與評估問卷中未符合之部分，做為組織強化個資管理整體準備度之參考方向。若屬於法律面之要求，則組織應立即採取行動方案以符合法律規定。各風險領域的分析範例，詳見圖 8。



資料來源： 本計畫整理

圖8　各風險領域個資管理整體準備度雷達圖(空白範例)

個資管理現況評估之任務，包括進行組織個資管理現況評估、分析個資管理現況評估資料及產出組織個資管理現況評估分析結果。有關每項任務內容，說明如下：

Ÿ　進行組織個資管理現況評估

組織可經由個資管理整體準備度評估問卷填寫作業，回答問卷內的項目為符合、不符合或不適用，並分別統計其數量，再繪製成雷達圖或其他圖形(如長條圖等)，即可初步瞭解目前組織於個資管理中，那一項風險領域是屬於較高部分。

Ÿ　分析個資管理現況評估資料

組織應就個資管理整體準備度評估問卷之統計結果，分析每項風險領域中的符合、不符合或不適用項目是否確實。例如，在「訓練」風險領域的評估細項問到：「組織對個人資料管理的教育訓練內容是否包括角色及職責之說明？」，回答內容若為「符合」，則應確認訓練內容是否屬實；若為「不符合」，則未來在規劃「控制措施」時，應納入考量；若為「不適用」，則

應瞭解其原因。

Ÿ 產出組織個資管理現況評估分析結果

最後的統計分析結果，建議以圖形方式呈現，並於個資管理會議中報告與核定，依分析結果執行後續作業。

以圖 9 為範例，該圖為組織在運用個資保護管理建置流程導入前，所進行之個資管理整體準備度評估結果，在流程構面上，對於個資作業的管理面上具有一定程度以上的準備度，在「資料蒐集與保存」、「利用與揭露」及「保護/安全性」等領域有較高的準備度，但相對觀察其他與個資整體框架有關領域，準備度則明顯偏低，甚至大部分幾乎都仍處於未開始至起始階段之間。

深入瞭解現況後，發現由於組織早已通過 CNS/ISO/IEC 27001 資訊安全管理與 ISO/IEC 20000 資訊服務管理系統制度驗證，因此在內部作業流程上已具備相當程度的準備度，在被動性的個資保護流程上便形成相當程度以上的效益。在安全技術方面，由於該組織已依資訊安全管理制度實施控制措施，因此也顯現出在這些評估領域之中具有較高的準備度。

不過在法令遵循性等方面，發現既有的資訊治理架構中尚欠缺對於個資法的著墨，因此，大部分屬於主動性的個資保護措施，例如隱私保護政策、適當的管理組織架構、隱私保護作業的人員職責定義與訓練、隱私告知原則及公開原則的實踐等，都處於急待提升的階段，這些將是組織在個資保護實作時，個資管理整體架構與流程面上的重點。

需注意的是，內部各單位對於應用於個資保護的技術措施或方案，需建立統一的做法或原則，依據個資項目衝擊評鑑結果，結合可行的個資保護技術方案，建立一套個資管理在安全技術措施實務上依循之參考基準。

資料來源： 本計畫整理

圖9　個資保護管理建置流程導入前個資管理整體準備度雷達圖範例

3.1.6. 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。

參考 BS 10012:2009 個人資訊管理系統標準之建議，組織可透過營運作業流程或服務目錄方式，對組織進行完整的個資盤點。

個資項目盤點之任務，包括識別不同作業流程之個資項目、識別個資項目之類別、依據及目的、識別個資項目相關生命週期活動、識別個資項目與外部利害關係人之關聯及完成個資項目盤點。有關每項任務內容，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 (詳見表 6)。

表6　個資流程分析表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		

資料來源： 本計畫整理

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，詳見表 7 與表 8。

表7　個資項目蒐集範圍

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	間接識別的欄位
服務目錄或流程名稱	子流程名稱																							

資料來源： 本計畫整理

表8　個資項目基本資料表

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別

資料來源： 本計畫整理

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。個資項目生命週期詳見表 9。

表9　個資項目生命週期

業務或服務作業流程		個人資料檔案名稱	個人資料檔案生命週期活動									
服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式

資料來源： 本計畫整理

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，詳見表 10。

表10 個資項目利害關係人

業務或服務作業流程		個人資料檔案名稱	利害關係人				
服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他

資料來源： 本計畫整理

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(詳見表 11)，做為後續個資衝擊分析與評鑑之依據。

表11 個資項目盤點表

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄 或 流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他

資料來源： 本計畫整理

3.1.7. 個資衝擊分析

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。

個資衝擊分析之任務，包括設計個資衝擊分析檢核表、進行個資項目個資衝擊分析及完成個資衝擊分析。有關每項任務內容，說明如下：

- 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，內容詳見附件 5「個資項目個資衝擊分析檢核表」。

- 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(詳見附件 6)。

- 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。

3.1.8. 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，做為後續擬定安全控制措施之依據。

個資風險評估之任務，包括設計個資項目之個資風險等級基準值、分析個資項目個資性之風險等級及完成個資風險評估。有關每項任務內容，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。個資風險等級基準值建議，詳見表 12。

表12 個資風險等級基準值建議表

參考項目	個資風險等級		
	普	中	高
含有個資類別	未具有任何個資，或僅含有姓名、公務電話、公務傳真、公務 email 等公務個資，且公務個資筆數不超過特定筆數(依機關需求自行訂定)	含有一般個資，如姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等「個人資料保護法」定義之個人資料數量在特定筆數(依機關需求自行訂定)以下，或公務個資數量超過特定筆數(依機關需求自行訂定)(含)以上	含有特種個資，如有關醫療、基因、性生活、健康檢查及犯罪前科之個資，或含有一般個資之資料筆數超過特定筆數(依機關需求自行訂定)(含)以上
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	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成有限的傷害(可能輕微影響本機關聲譽、但不會造成任何財務損失或遭受訴訟之情事)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成傷害(可能會影響本機關聲譽、財務損失或遭受訴訟，但不至於對本機關業務之持續運作造成重大影響)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成重大傷害(非常可能嚴重影響本機關聲譽、重大財務損失或重大訴訟，且可能造成本機關主要業務中止)
「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	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為普或安全等級為中者不超過一項	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面的安全等級皆無高，且其中二項安全等級為中	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為中，或「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信

			譽」三者影響構面之其中一項安全等級為高者

資料來源： 本計畫整理

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，詳見表 13。

表13 PIA/RA 安全控制項目基準值

業務或服務作業流程		個人資料檔案名稱	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	「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
服務目錄或流程名稱	子流程名稱				

資料來源： 本計畫整理

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，詳見表 14，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。

表14 個資項目個資風險評估表

業務或服務作業流程			個人資料檔案名稱	PIA/RA 安全控制項目基準值			個資性之風險等級
編號	服務目錄或流程名稱	子流程名稱		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	「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	

資料來源： 本計畫整理

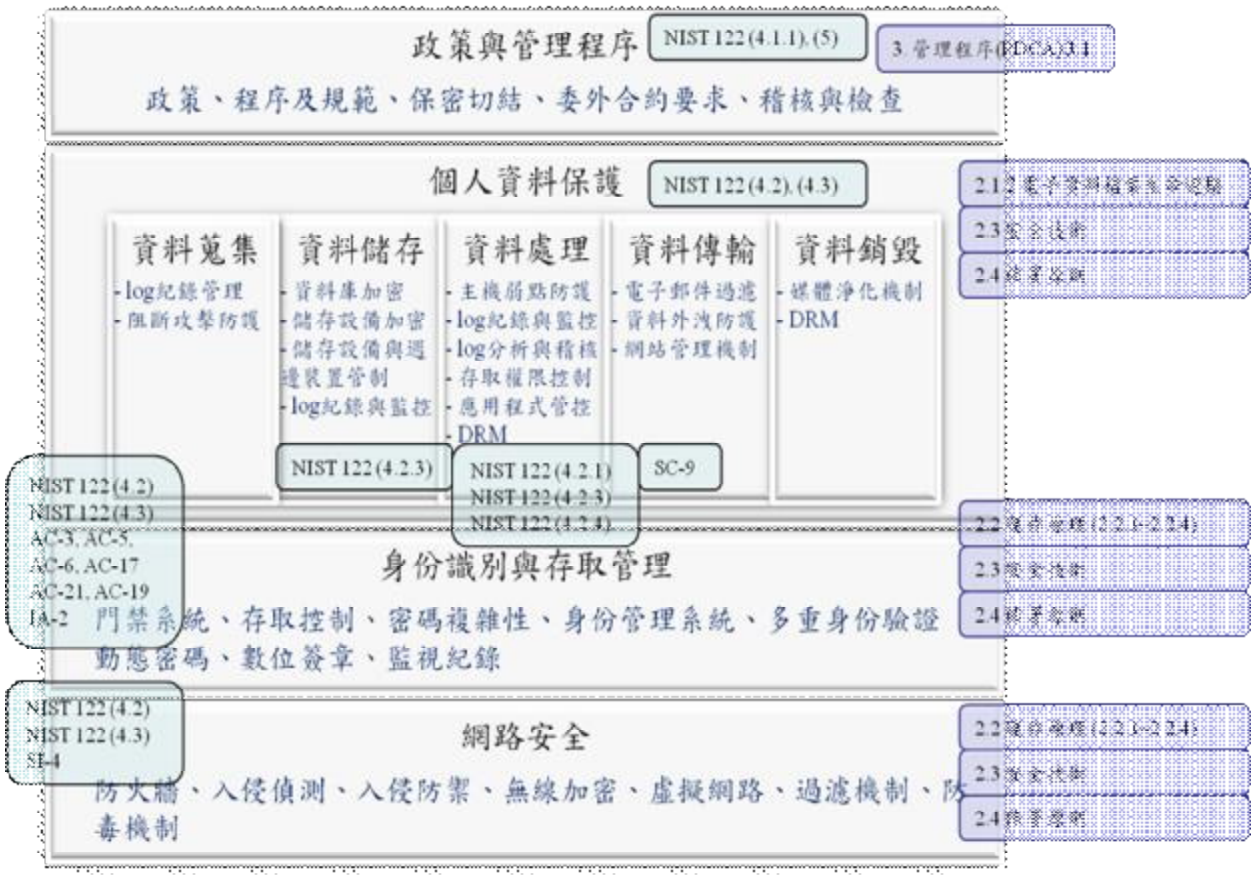
3.1.9. 安全控制措施規劃

安全控制措施規劃，係依據個資風險評估對於組織所擁有個資項目不同的風險等級，規劃不同風險等級個資保護技術方案與控制方法。

安全控制措施規劃之任務，包括規劃組織安全控制措施、評估所需資源及確認組織安全控制措施規劃內容。有關每項任務內容，說明如下：

Ÿ 規劃組織安全控制措施

個資管理之防護技術架構，包括對於個資保護生命週期不同階段活動之安全措施項目、整體環境之身分識別與存取管理以及基礎設施網路安全管理等，整體架構詳見圖 10。



資料來源： 本計畫整理

圖10 個資管理防護技術架構

依此架構，參考美國國家標準與技術局訂定之 NIST SP800 系列資訊安全相關指引(包括 NIST SP800-122 個人可識別資訊機密性保護指引、NIST

SP800-53 安全控制指引)、CNS/ISO/IEC 27001 資訊安全管理標準及「電子資料保護參考指引」，並參考 NIST SP800-122 安全控制之普、中、高分級，綜整為個資保護技術安全控制項目基準值建議。個資保護技術安全控制項目與參考指引對照，詳見表 15。各類別技術安全控制項目與個資法條款對照，詳見表 16。個資保護技術安全控制項目基準值建議，詳見表 17 惟本基準值係屬建議性質，如有不足之處，組織應依實際需求，新增所需之技術控制措施。

表15 個資保護技術安全控制項目與參考指引對照表

NIST 安全控制代碼	NIST 安全控制名稱	安全控制說明	參考指引
AC-3	存取控制機制	機關可透過對存取控制政策的建構及存取控制機制(例如使用存取控制表)，以達到控制個資存取的目的。控制存取之執行還包括對儲存資料的加密，以防止因遺失可攜式行動裝置而導致個人資料外洩的嚴重後果	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 ▪ 2.3 安全技術 安全控制措施參考指引 V.2 ▪ 9 實體與環境安全 ▪ 11 存取控制 ▪ 15 遵循性
AC-5	職務區隔	機關在設計存取個資的控制時，亦可採用職務區隔的概念，將工作流程於資訊系統中適當切割，以避免違反獨立性原則的情況發生	電子資料保護參考指引 V.2 ▪ 2.1.3 電子資料分類分級 安全控制措施參考指引 V.2 ▪ 6 資訊安全的組織 ▪ 11 存取控制 ▪ 12 資訊系統獲取、開發及維護
AC-6	最小權限	機關應要求其使用者在執行某項(些)業務時，僅使用與業務相關的最小權限及功能(例如讀、寫、執行)，同時並確認使用者僅能接觸最低數量的個資	電子資料保護參考指引 V.2 ▪ 3.3.3 處理 安全控制措施參考指引 V.2 ▪ 7 資產管理 11 存取控制
AC-17	遠端存取	機關可採用禁止或限制遠端存取的方式，控制對個資的接觸。對於核准之遠端存取，亦要確認個資在傳輸過程中予以妥善加密	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 安全控制措施參考指引 V.2 ▪ 11 存取控制
AC-21	使用者基礎的協同合	機關於提供合約規範下的資訊共享時，應使用自動控制機制比對(確認)存取授權符合存取控制	電子資料保護參考指引 V.2 ▪ 3.3.6 流通

NIST 安全控制代碼	NIST 安全控制名稱	安全控制說明	參考指引
	作與資訊分享		
AC-19	可攜式與行動設施的存取控制機制	機關對於禁止或限制個資的存取，可透過對可攜式行動裝置的使用控制來達成。由於其便於攜帶的特質，較桌上型電腦更容易產生遺失資料的風險。部分組織採取有限度地使用可攜式行動裝置。當進行遠端存取重要個資時，應確認高風險之個資不會離開機關實體保護範圍。即使個資之遠端存取經過授權核准，機關也會確認所使用之行動裝置受到適當的保護與定期接受掃描	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 ▪ 2.3.5 存取控制 ▪ 3.3.4 傳送 安全控制措施參考指引 V.2 ▪ 9 實體與環境安全 ▪ 11 存取控制
AU-2	稽核事件	機關可透過稽核事件及早發現因未經授權而存取個資的行為所造成的個資外洩情形	電子資料保護參考指引 V.2 ▪ 2.3.6 稽核 ▪ 3.3.7 技術控制措施 安全控制措施參考指引 V.2 ▪ 11 存取控制 ▪ 13 資訊安全事故管理
AU-6	稽核紀錄的監控、分析及報告	機關可透過定期資訊系統稽核、稽核資料分析和報告適當層級主管，以及早發現與處理違反個資安全之異常行為	電子資料保護參考指引 V.2 ▪ 3.4 測試「檢查」Check ▪ 3.5 整合「行動」Act
IA-2	識別與鑑別(機關使用者)	使用者於存取個資時應透過適當的識別與證明使用者身分。識別方式的強度取決於個資的重要性，例如美國聯邦政府要求個資遠端存取應採用二元識別方式(two-factor authentication)，並需於帳號於一段時間未使用後重新登入	電子資料保護參考指引 V.2 ▪ 3.3.7 技術控制措施 電子身分認證參考指引
MP-2	媒體存取	機關可限制個資透過媒體存取，媒體亦包括具有資料儲存能力之可攜式行動裝置	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 ▪ 3.3.5 儲存 安全控制措施參考指引 V.2 ▪ 9 實體與環境安全 ▪ 10 通訊與作業管理
MP-3	媒體標記	機關應明確標示存有個資的電子或非電子媒體，並規劃媒體應如何處理與配置。	電子資料保護參考指引 V.2 ▪ 2.1.3 電子資料分類分級 ▪ 2.1.4 電子資料生命週期 安全控制措施參考指引 V.2 ▪ 7 資產管理 ▪ 9 實體與環境安全
MP-4	媒體儲	機關應確認妥善存放儲有個資的電子及非電	電子資料保護參考指引 V.2

NIST 安全控制代碼	NIST 安全控制名稱	安全控制說明	參考指引
	存	子媒體。這些媒體經確認不再使用後，應使用適當技術、方式及流程予以適當銷毀或消磁	▪ 2.1.4 電子資料生命週期 ▪ 3.3.5 儲存 安全控制措施參考指引 V.2 ▪ 9 實體與環境安全
MP-5	媒體運輸	機關應確認存有個資的電子及非電子媒體，於機關之外運輸時能得到妥善的保護，譬如將存有個資之資料進行加密或將媒體存放於上鎖的運送箱等方式	電子資料保護參考指引 V.2 ▪ 3.3.6 流通 安全控制措施參考指引 V.2 ▪ 9 實體與環境安全
MP-6	媒體淨化	機關對存有個資之電子及非電子媒體於報廢或回收加工時應確認妥善處理。例如對電子媒體要確認其已被徹底消磁	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 安全控制措施參考指引 V.2 ▪ 10 通訊與作業管理
SC-9	傳輸機密性	為確保個資保密及防止個資外洩，機關於個資傳輸前，應確認其已經過妥善加密	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 ▪ 3.3.6 流通 安全控制措施參考指引 V.2 ▪ 10 通訊與作業管理
SC-28	靜態資訊的保護	機關對於儲存於硬碟及備份媒體中的個資應以適當方式予以加密，以達成個資保密及防止外洩的目標	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 安全控制措施參考指引 V.2 ▪ 10 通訊與作業管理
SI-4	資訊系統監視	機關應適當監控其資訊系統及內部網絡，以即時偵測個資於內部網路之異常傳輸	電子資料保護參考指引 V.2 ▪ 2.1.4 電子資料生命週期 安全控制措施參考指引 V.2 ▪ 10. 通訊與作業管理 ▪ 12 資訊系統獲取、開發及維護

資料來源： 本計畫整理

表16 各類別技術安全控制項目與個資法條款對照表

技術安全控制項目類別	個資法條款
存取控制機制	§11(維持資料之正確性)
	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(指定專責人員與安全維護)
職務區隔	§11(維持資料之正確性)
	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(指定專責人員與安全維護)
最小權限	§15(資料之蒐集與處理)
	§16(資料之利用)
遠端存取	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(安全維護)
使用者基礎的協同合作與資訊分享	§11(維持資料之正確性)
	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(安全維護)
可攜式與行動設施的存取控制機制	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(安全維護)
稽核事件	§18(安全維護)
稽核紀錄的監控、分析及報告	§11(維持資料之正確性)
識別與鑑別(機關使用者)	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(安全維護)
媒體存取	§15(資料之蒐集與處理)
	§16(資料之利用)
	§18(安全維護)
媒體標記	§17(資料之公開)
媒體儲存	§18(安全維護)
媒體運輸	§15(資料之蒐集與處理)
	§16(資料之利用)
媒體淨化	§11(維持資料之正確性)
	§18(安全維護)
傳輸機密性	§15(資料之蒐集與處理)

	§16(資料之利用)
靜態資訊的保護	§18(安全維護)
資訊系統監視	§18(安全維護)

資料來源： 本計畫整理

表17 個資保護技術安全控制項目基準值建議表

安全控制(NIST 編號)	風險等級所對應之安全控制項目基準值建議		
	普	中	高
存取控制機制(AC-3)	▪ 應建立個資處理授權表、亦應將加密應用於設備、檔案、紀錄、程式、網域等存取活動 ▪ 應建立應用層(application level)之存取控制 ▪ 應依據機關訂定之密碼原則做為最低設定標準 ▪ 除因執行業務所需外，應啟動逾時未操作之密碼保護設定(如啟用螢幕保護密碼、session time out 等) ▪ 使用者應啟動瀏覽器安全設定，以限制執行非信任網站之行動碼	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 依據風險評估結果與人員職責，應開放必要之最小權限(除可執行之應用程式、系統功能外，亦包括可使用之通訊埠(port)、通訊協定(protocol)及服務(services))；或建議結合職務區隔 ，採用以角色為基礎的存取控制(Role-based access control)機制 ▪ 建議採用資料外洩防護(Data Loss Prevention，以下簡稱DLP)工具，管理使用者傳送個資或機密資料之行為 ▪ 若需要與外單位交換個資則建議採用數位版權管理(Digital Right Management, 以下簡稱 DRM)工具，以限定個別使用者之存取權限	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 應採用 DLP 與 DRM 工具，若本項個資均為特種個資，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機關資安規範之行為
職務區隔(AC-5)	無建議	▪ 應依據獨立性原則採用職務區隔 (separation of duties)，譬如負責系統管理者(如administrator)不應同時負責管	▪ 請參閱本控制項基準值為「中」之控制措施

		理系統日誌(log) ▪ 職務區隔 應應用於系統管理、程式開發、組態管理、系統測試、網路管理等活動，並建議結合存取控制，採用以角色為基礎的存取控制(Role-based access control)機制，相關方案請參閱「存取控制機制(AC-3)」基準值為「中」之控制措施說明 ▪ 執行存取控制者不得稽核自身相關工作 ▪ 系統管理角色應分開使用管理者帳號，而非全部使用最高權限(如 administrator)或僅使用單一帳號(譬如系統管理可分為 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)	
最小權限(AC-6)	無建議	▪ 請參閱「職務區隔 (AC-5)」基準值為「中」之控制措施說明	▪ 請參閱本控制項基準值為「中」之控制措施
遠端存取(AC-17)	▪ 遠端存取管制範圍除與機關之外部連線外，亦包括使用者於機關非使用本機登入，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)連線至機關資訊系統之存取活動，存	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 機關應建立遠端存取之自動監控措施以確保從遠端連線至機關資訊系統之活動均符合機關所訂定之遠端存取政策 ▪ 遠端存取應使用加密線路以確保傳輸資料之機密性與完整性	▪ 請參閱本控制項基準值為「中」之控制措施

	取控制原則與政策請參考「存取控制機制 (AC-3) 」基準值為「普」之控制措施說明	▪ 建議遠端存取透過 VPN 連線	
使用者基礎的協同合作與資訊分享 (AC-21)	無建議	▪ 個資不應儲存於共享資料夾 ▪ 權限可依據個人、組別、組織等層級進行功能分類與授權，譬如限制讀取、寫入、刪除、執行、列印等 ▪ 建議可使用 DLP 與 DRM 工具，請參閱「存取控制機制 (AC-3)」基準值為「中」之控制措施 ▪ 儲存於資料庫之密碼與敏感/特種個資應運用雜湊函數 (hash)之輸出值儲存資料	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 儲存於資料庫之密碼與機密/特種個資建議採用 SHA-1 雜湊演算法之輸出值儲存
可攜式與行動設施的存取控制機制 (AC-19)	▪ 可攜式行動裝置包括外接儲存設備(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/通訊設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等) ▪ 以上裝置若連接至機關內部網路與資訊系統時應經過授權始可使用，並應符合機關資訊安全原則 ▪ 若人員需要攜出屬於機關之可攜式裝置(譬如出差或外出執行公務等)，回來的時候應該要檢查	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 機關應限制可寫入與可攜式媒體之使用(僅授權人員得使用) ▪ 機關應禁止使用私有之可攜式媒體 ▪ 機關應禁止無特定保管者之可攜式媒體的使用 ▪ 建議可使用 DLP 與 DRM 工具，請參閱「存取控制機制 (AC-3)」基準值為「中」之控制措施	▪ 請參閱本控制項基準值為「中」之控制措施

	曾去的地方是否屬於高風險、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		
稽核事件(AU-2)	無建議	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 具有最高或特殊權限之使用者或其授權使用之系統功能應設定事件稽核日誌(event log) ▪ 機關應指派專人定期審視事件稽核日誌(event log) ，且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 ▪ 若事件稽核日誌包括敏感/特種個資內容，則應加密處理，僅負責審視或稽核該日誌者得存取完整內容	▪ 請參閱本控制項基準值為「中」之控制措施
稽核紀錄的監控、分析及報告(AU-6)	▪ 機關應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 ▪ 若機關有資訊資產、組態項目、資產、人員或組織形態有重大變更時，或是個資法條文有異動時，應重新審視個資管理稽核計畫與頻率，並視需要進行調整	▪ 請參閱本控制項基準值為「普」之控制措施	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 應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機關相關人員進行調查與回應

識別與鑑別(機關使用者）(IA-2)	▪ 使用者帳號應具有唯一鑑識性(使用者包括機關正職員工、約聘員工、顧問等) ▪ 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 ▪ 使用者身分認證方式包括使用者帳號、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 ▪ 使用者身分識別應應用於系統本機端存取(local access)與遠端存取(包括透過 LAN、WAN 或 VPN 等方式)	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 所有使用者透過遠端登入時，應使用二元識別或多元識別之認證 ▪ 資訊系統之最高權限或特殊權限使用者於本機登入時，應使用二元識別或多元識別之認證 ▪ 資訊系統之最高權限或特殊權限使用者透過遠端登入時，應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	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 所有使用者無論於本機或遠端登入時，應使用二元識別或多元識別之認證 ▪ 所有使用者於遠端登入時，應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 ▪ 傳送電子文件(包括電子郵件)時應使用數位簽章

媒體存取(MP-2)	▪ 資訊系統媒體包括電子媒體(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) ▪ 本控制項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)	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 機關應設置具有實體安全控管之環境存放備份媒體，且應嚴禁非授權存取備份媒體 ▪ 建議可使用 DLP 與 DRM 工具，請參閱「存取控制機制(AC-3)」基準值為「中」之控制措施	▪ 請參閱本控制項基準值為「中」之控制措施
媒體標記(MP-3)	無建議	▪ 個資等級標示範圍應包括應用系統與資訊系統媒體(相關定義請參考「媒體存取(MP-2)」控制措施說明) ▪ 書面文件等級建議將等級標示於文件封面、封底或以浮水印的方式呈現	▪ 請參閱本控制項基準值為「中」之控制措施
媒體儲存(MP-4)	無建議	▪ 本控制項應包括資訊系統媒體(相關定義請參考「媒體存取(MP-2)」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) ▪ 存放儲存個資儲存媒體之場所應設有實體管控措施，並限制可接觸該媒體之人員 ▪ 個資應加密後進行儲存，加密強度應依據個資機密和完整性等級設定	▪ 請參閱本控制項基準值為「中」之控制措施

媒體運輸 (MP-5)	無建議	▪ 本控制項應包括資訊系統媒體、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) ▪ 應限制負責傳輸或傳送存有個資儲存媒體之人員 ▪ 個資儲存媒體於傳送時所使用之包覆措施應具有實體管控措施，如密封盒、可上鎖之儲物箱等 ▪ 個資應加密後儲存，加密強度應依據個資機密和完整性等級設定 ▪ 個資儲存媒體運送時應記錄儲存媒體識別資料(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 ▪ 若個資儲存媒體需委外傳送(譬如透過郵局、快遞公司等)，應加強其包覆措施之強度，並留下相關紀錄	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 機關應指派專人負責遞送個資儲存媒體
媒體淨化 (MP-6)	▪ 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)方式包括媒體清除(clear)、刪除(purge)及破壞(destory) ▪ 應依據個資機敏等級選擇適當的儲存媒體淨化方式，建議如下 – 電子儲存媒體應採	▪ 請參閱本控制項基準值為「普」之控制措施 ▪ 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，且應限制僅能提供機關內部人員使用；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	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 機關應追蹤、記錄並核對儲存媒體淨化與銷毀程序 ▪ 機關應定期測試儲存媒體淨化設備與程序是否正常運行 ▪ 機關應於使用資訊系統媒體與可攜式行動裝置前先進行媒體淨

	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，譬如含個資之文件應攪碎或透過水銷、焚燒等方式銷毀	– 非電子儲存媒體則應透過水銷或焚燒方式銷毀	化程序以避免惡意程式感染機關之資訊系統 ▪ 電子儲存媒體若需重複使用必須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；其於則請參考本控制項基準值為「中」之控制措施
傳輸機密性(SC-9)	無建議	▪ 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，應用程式包括 e-mail、FTP 等 ▪ 機關於資料傳輸時應進行加密 ▪ 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 ▪ 若需使用無線網路，則應使用加密連線	▪ 請參閱本控制項基準值為「中」之控制措施 ▪ 禁止使用無線網路傳輸此等級之資料
靜態資訊的保護(SC-28)	無建議	▪ 本控制項適用於硬碟與儲存媒體 ▪ 請參閱「媒體淨化(MP-6)」基準值為「中」之控制措施	▪ 請參閱本控制項基準值為「中」之控制措施
資訊系統監視(SI-4)	無建議	▪ 應建置可偵測資訊系統攻擊事件之監控與防護工具，其中可分為內部和外部，內部包括	▪ 請參閱本控制項基準值為「中」之控制措施

		系統監視、內部網路或系統元件之間的事件偵測工具，外部則包括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。 ▪ 建議設置以下工具協助進行網路監控與防護： – 防火牆(firewall) – 入侵偵測系統(IDS) – 入侵防禦系統(IPS) – 惡意軟體偵測(如防毒軟體、防木馬間諜軟體等) – 電子郵件/網路瀏覽內容安檢軟體(MIMESweeper、Spam filter等) ▪ 資訊系統監視工具應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 ▪ 資訊系統監視工具應架設於機關與外部網路連接界限、重要伺服器(server farm) 與內部網路界限 ▪ 機關使用之自動化監測工具，應具有偵測內送(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，譬如偵測惡意程式或異常大量傳送之封包 ▪ 機關使用之自動化監測工具應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 ▪ 自動化監測工具若需自行設定政策、過濾條件(如firewall、MIMESweeper 等)，應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。 ▪ 資訊系統應定期執行滲透測試與弱點掃描測試，並針對中、高風險(至少)之測試掃描結果進行改善 ▪ 自行開發之系統應執行原始碼檢測，檢測項目至少包括OWASP Top 10 等著名安全問題	

資料來源： 本計畫整理

組織可依應處理之衝擊與個資風險等級，參考個資保護技術安全控制項目基準值建議，研擬所需之安全控制措施。

Ÿ 評估所需資源

組織應依據衝擊影響層面排定優先處理順序，再依組織個人資料保護管理要點、個資衝擊分析及個資風險評估所評估之個資風險等級，參考個資保護安全控制項目基準值建議表與「電子資料保護參考指引」，考量組織所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，評估在有限資源下，需優先進行處理之安全控制措施，並列出要達到此業務目標與需求之安全控制措施所需資源。

Ÿ 確認組織安全控制措施規劃內容

組織應依規劃所需之安全控制措施，排除組織目前已實作或已計畫實施中之控制措施，檢查所有應處理之衝擊，是否皆有合適之安全控制措施或應加強之安全控制措施，並訂定未來應建立之安全控制措施，經核定後做為實作安全控制措施依據。

3.2.執行

執行階段為組織於評量個資整體環境、衝擊分析及衝擊評鑑後，依上階段的規劃結果，執行各項個資管理措施。

本階段之活動，包括確立人員權責角色、建立個資管理程序、建立安全控制措施、個資委外作業管理及宣導與教育訓練，有關本階段之輸入項目、產出項目及執行手法與相關工具，詳見表 18，分述如下：

表18 執行階段活動與任務表

活動與任務 (ACTIVITY & TASK)	輸入項目 (INPUT)	產出項目 (OUTPUT)	執行方法與相關工具 (TECHNIQUE & TOOL)
Activity1：確立人員權責角色			
Task1：識別個資管理相關人員或群組角色	組織架構圖、與個資有關之利害關係人清單	個資管理角色一覽	資料蒐集與分析
Task2：建立個資項目生命週期活動與個資管理角色之對應表	個資項目盤點表	個資項目與個資管理角色對應表	人員訪談、個資項目與個資管理角色對應表範例
Task 3：識別對應表內個資管理角色細部權責定義需求	個資項目與個資管理角色對應表		資料蒐集與分析、人員訪談
Task 4：完成人員權責角色定義	個資項目與個資管理角色對應表	個資項目與個資管理角色對應表	資料蒐集與分析、個資項目與個資管理角色對應表範例
Task 5：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	個資項目與個資管理角色對應表	(相關應用系統權限設定/申請單)	(相關應用系統權限設定/申請單範例)
Activity 2：建立個資管理程序			
Task 1：設計個資生命週期作業流程	個資項目盤點表、 作業流程或管理制度程序書	個資生命週期作業流程	流程圖範例、個資提供同意書範例、隱私權政策範例、個人資料異動申請書範例、個人資料調閱申請書範例
Task 2：設計個資事故管理作業流程	個資作業流程圖與作業程序、資安事故通報與作業程序書	個資事故管理作業流程圖	流程圖範例、個資事故通報與紀錄表範例

活動與任務 (ACTIVITY & TASK)	輸入項目 (INPUT)	產出項目 (OUTPUT)	執行方法與相關工具 (TECHNIQUE & TOOL)
Task 3：設計個資管理稽核作業流程	個資作業流程圖與作業程序、內部稽核程序書	個資內部稽核作業程序	資料分析、稽核計畫範例、稽核紀錄表範例
Task 4：修訂組織內部管理制度文件	個資作業流程圖與作業程序、內部管理制度文件	修訂後內部管理制度文件	資料分析、組織內部管理制度文件管制暨發行辦法
Activity3：建立安全控制措施			
Task1：分析個資保護技術安全控制項目基準值需求	個資風險評估報告、個資保護技術安全控制項目基準值建議表	個資保護技術安全控制項目基準值需求	資料分析、個資保護安全控制項目基準值建議表、個資管理防護技術架構圖
Task 2：規劃個人資料生命週期保護構面控制項目行動方案	個資保護技術安全控制項目基準值需求	相關行動方案計畫、經費預算表	資料蒐集與分析、個資保護安全控制項目基準值建議表、經費預算
Task 3：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	個資保護技術安全控制項目基準值需求	相關行動方案計畫、經費預算表	資料蒐集與分析、個資保護安全控制項目基準值建議表、經費預算
Task 4：規劃基礎設施網路安全管理構面控制項目行動方案	個資保護技術安全控制項目基準值需求	相關行動方案計畫、經費預算表	資料蒐集與分析、個資保護安全控制項目基準值建議表、經費預算
Task 5：建置個資保護技術安全控制項目行動方案	相關行動方案計畫、經費預算	(建置完成之行動方案)	個資保護技術安全控制項目基準值建議表
Activity4：個資委外作業管理			
Task 1：檢視個資委外作業契約	個資項目盤點表、 契約書	個資委外作業契約書	委外合約個資保護條款範例、保密切結書個資保

活動與任務 (ACTIVITY & TASK)	輸入項目 (INPUT)	產出項目 (OUTPUT)	執行方法與相關工具 (TECHNIQUE & TOOL)
與範圍		與工作計畫書	護條款範例
Task 2：調整個資委外作業契約與工作計畫書內容	個資委外作業合約書與工作計畫書	修正後之個資委外作業契約書與工作計畫書	委外合約個資保護條款範例、保密切結書個資保護條款範例
Task 3：規劃個資委外作業稽核計畫	修正後之個資委外作業契約書與工作計畫書、個資內部稽核作業程序	個資委外作業稽核計畫	稽核計畫範例、稽核紀錄表範例
Task 4：執行個資委外作業稽核	個資委外作業稽核計畫	個資委外作業稽核紀錄	個資管理紀錄蒐集、實地稽核、稽核紀錄表範例
Activity 5：宣導與教育訓練			
Task 1：規劃個資認知宣導活動	個人資料保護管理要點與風險處理計畫	組織安全控制措施原則	個資認知宣導海報範例
Task 2：規劃個資管理認知與教育訓練計畫	個資管理程序、安全控制措施、委外作業、稽核計畫	年度個資管理認知與訓練計畫、訓練教材	年度個資管理認知與訓練計畫表範例
Task 3：執行個資管理認知與教育訓練計畫	年度個資管理認知與訓練計畫、訓練教材	訓練紀錄、課程評量與回饋	年度個資管理認知與訓練計畫表範例

資料來源： 本計畫整理

3.2.1. 確立人員權責角色

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。

確立人員權責角色之任務，包括識別個資管理相關人員或群組角色、建立個資項目生命週期活動與個資管理角色之對應表、識別對應表內個資管理角色細部權責定義需求、完成人員權責角色定義及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。有關每項任務內容，說明如下：

- 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。

- 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，詳見表 19。

表19 個資項目與個資管理角色對應表

個資管理角色／個人資料檔案	計畫承辦窗口							單位秘書							文件管理人員							委外廠商窗口						
	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

資料來源： 本計畫整理

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。

3.2.2. 建立個資管理程序

為因應個資法之要求，組織需訂定個資保護政策，宣告對外網站之隱私權保護政策，明確規範內部的保護機制，檢視組織內部現行管理制度是否符合個資保護要求，同時一併檢討修正現行管理制度相關之程序書與執行表單。

組織於業務作業需求需蒐集個資時，應訂定個資蒐集作業流程，確認個資蒐集符合特定目的，同時設計個資同意書範本，以利於蒐集個資時使用。於蒐集資料之流程中，檢視所涉及之管理作業流程與程序書，符合組織之個資保護政策，修訂相關文件資料內容。本階段之管理重點為清楚的管理權責定義、依據法令與流程進行個資分類及落實公開與告知等隱私管理原則。例如針對短期持有(如行銷或抽獎目的)的個人資料，應透過蒐集程序告知當事人後續的個資處理與利用方式；當業務終止時，該項業務所擁有的個人資料是否依刪除／銷毀／淨化程序處理；對於久未利用或是太舊的個資，應檢討是否透過蒐集程序取得，並視檢討結果決定是否補行告知當事

人，以取得個資的後續處理與利用，或依刪除／銷毀／淨化程序處理等。

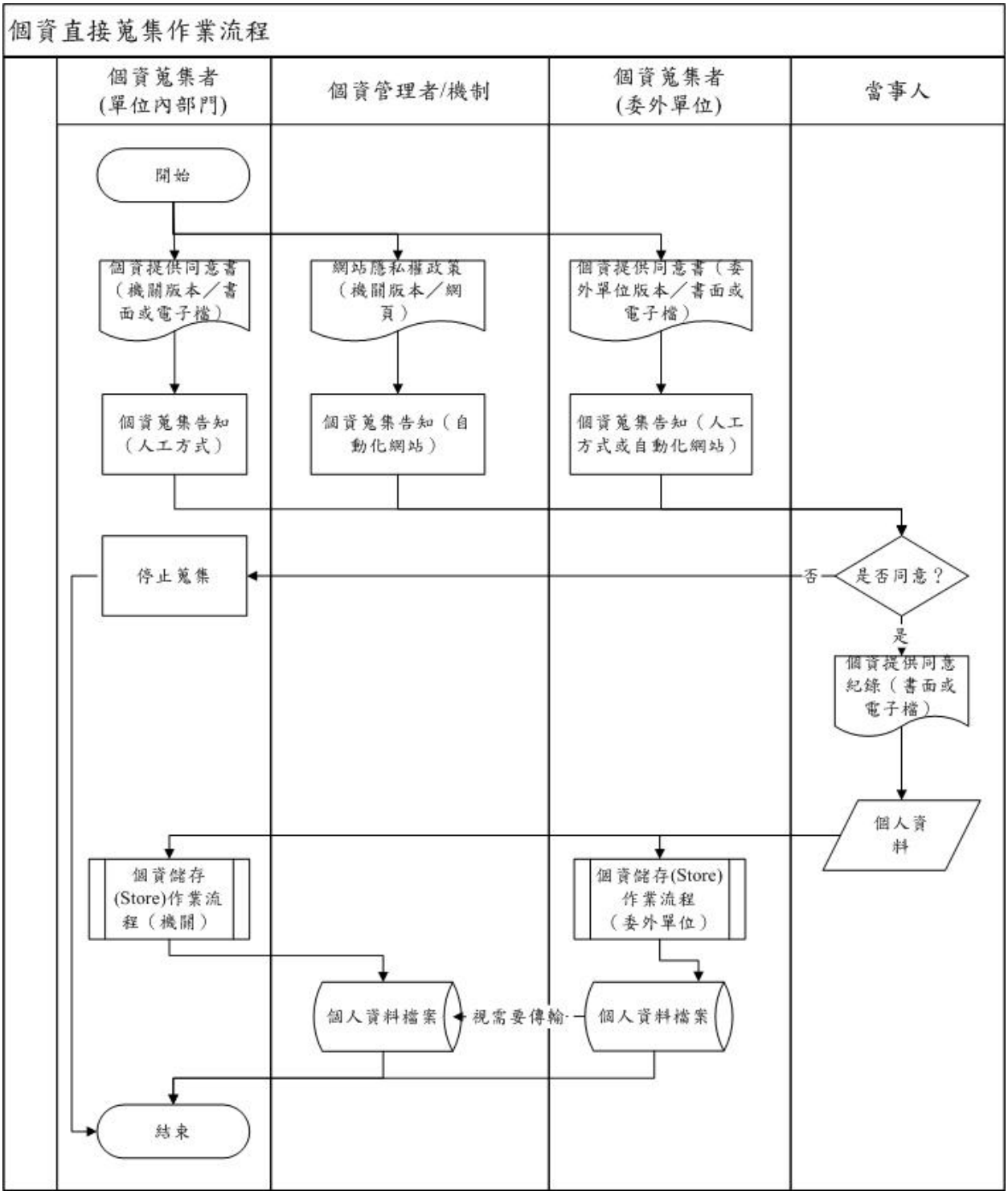
建立個資管理程序之任務，包括設計個資生命週期作業流程、設計個資事故管理作業流程、設計個資管理稽核作業流程及修訂組織內部管理制度文件。有關每項任務內容，說明如下：

Ÿ 設計個資生命週期作業流程

在施行細則規定之必要措施中，必須設計「個資資料蒐集、處理及利用之內部管理程序」。因此，組織應就所擁有的個資項目，設計相關作業流程，並調整相關管理作業程序書與使用人員權限，有效管制處理階段之個資安全。

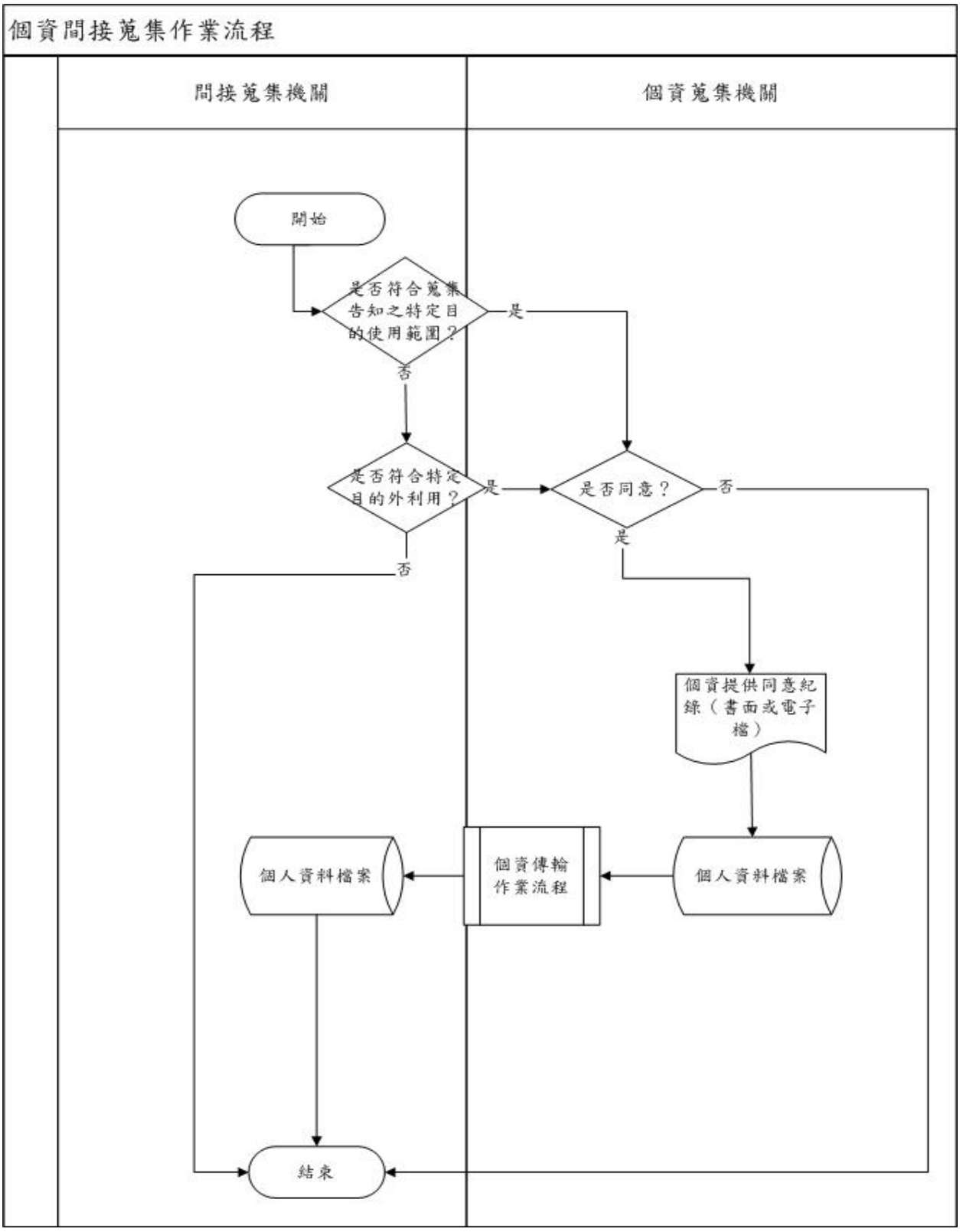
機關於業務執行過程中，有時會要求其他機關提供所擁有之個資資料，因而於個資蒐集流程中區分為直接與間接蒐集流程，以提供這兩種個資蒐集流程之區別，詳見圖 11 與圖 12。另外，個資資料於使用年限到期時，除進行個資資料刪除外，建議應執行媒體淨化作業，以確保刪除之資料已完全銷毀，詳見圖 17。

有關個資生命週期之說明可參考 3.2 規劃之「識別個資項目相關生命週期活動」，瞭解個資生命週期之各項活動後，即可設計其作業流程，詳見圖 11~圖 17。



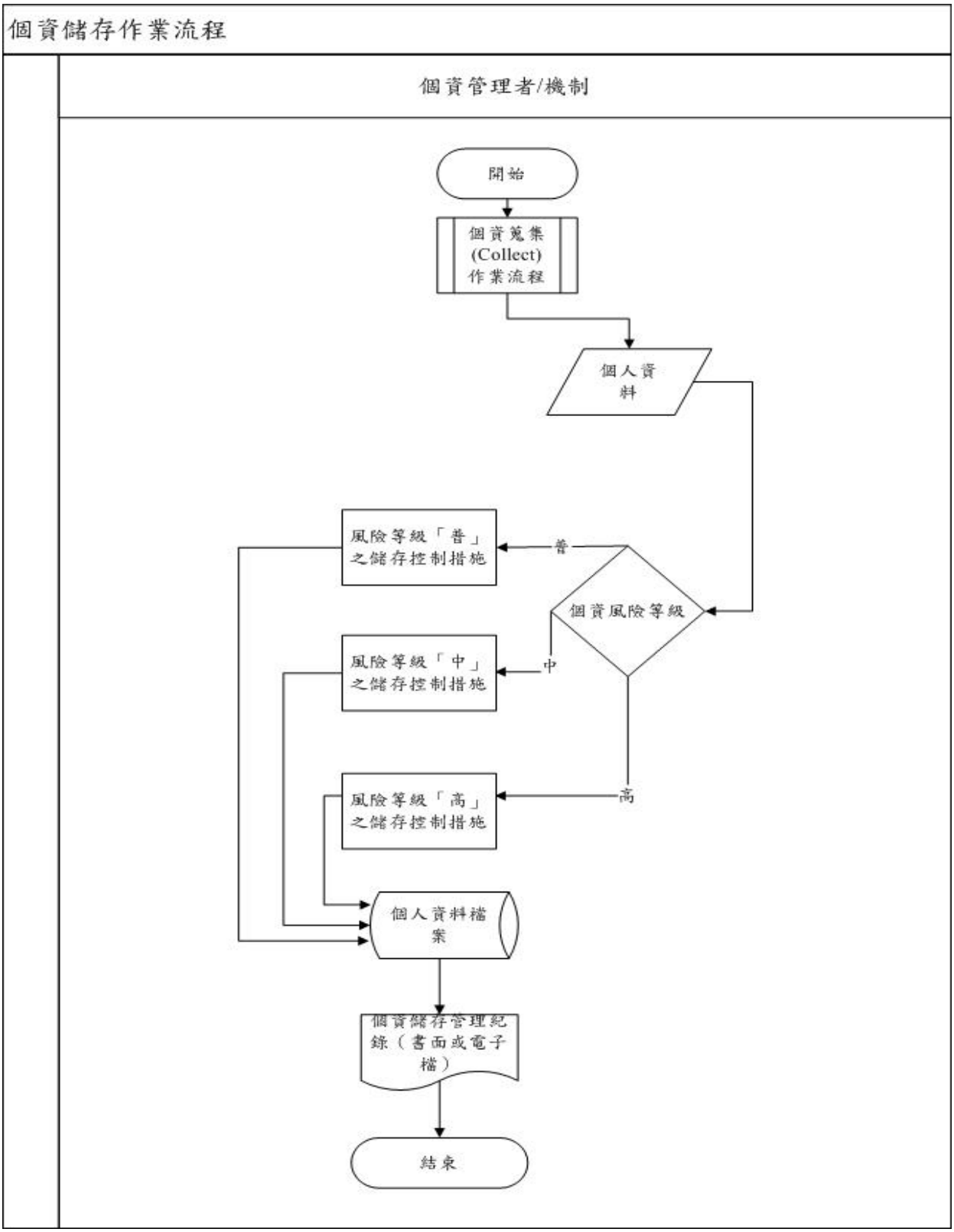
資料來源： 本計畫整理

圖11 個資直接蒐集作業流程範例



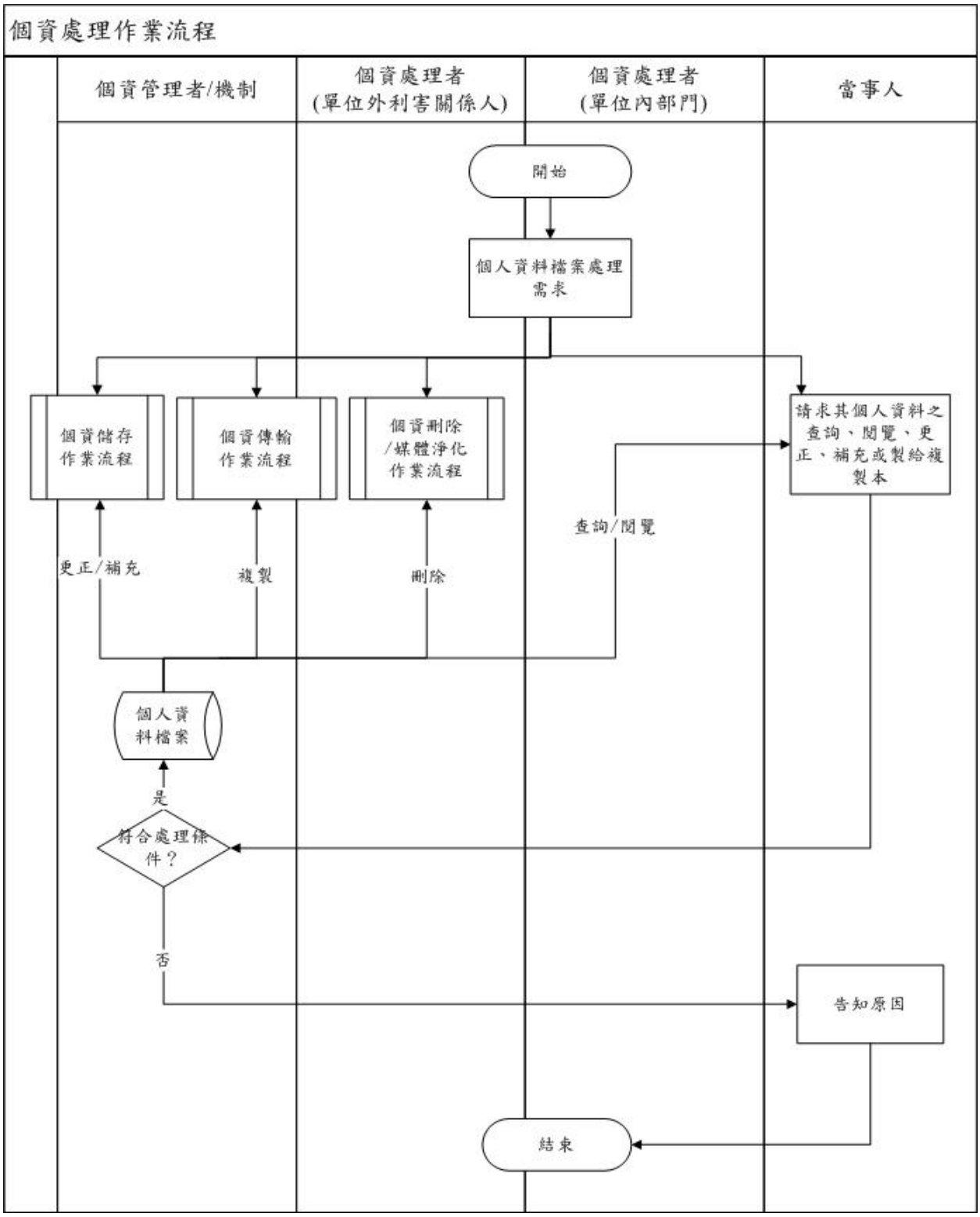
資料來源： 本計畫整理

圖12 個資間接蒐集作業流程範例



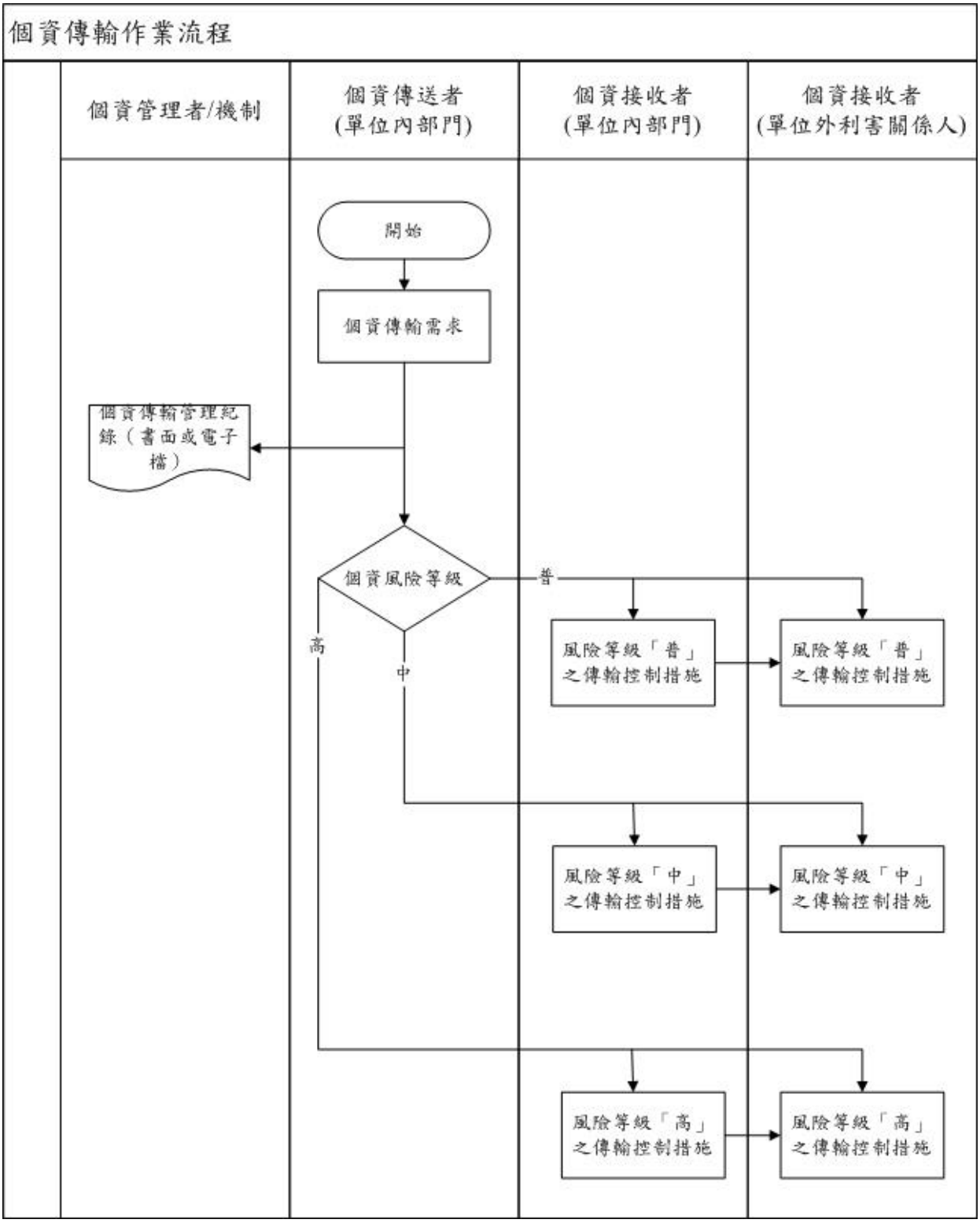
資料來源： 本計畫整理

圖13 個資儲存作業流程範例



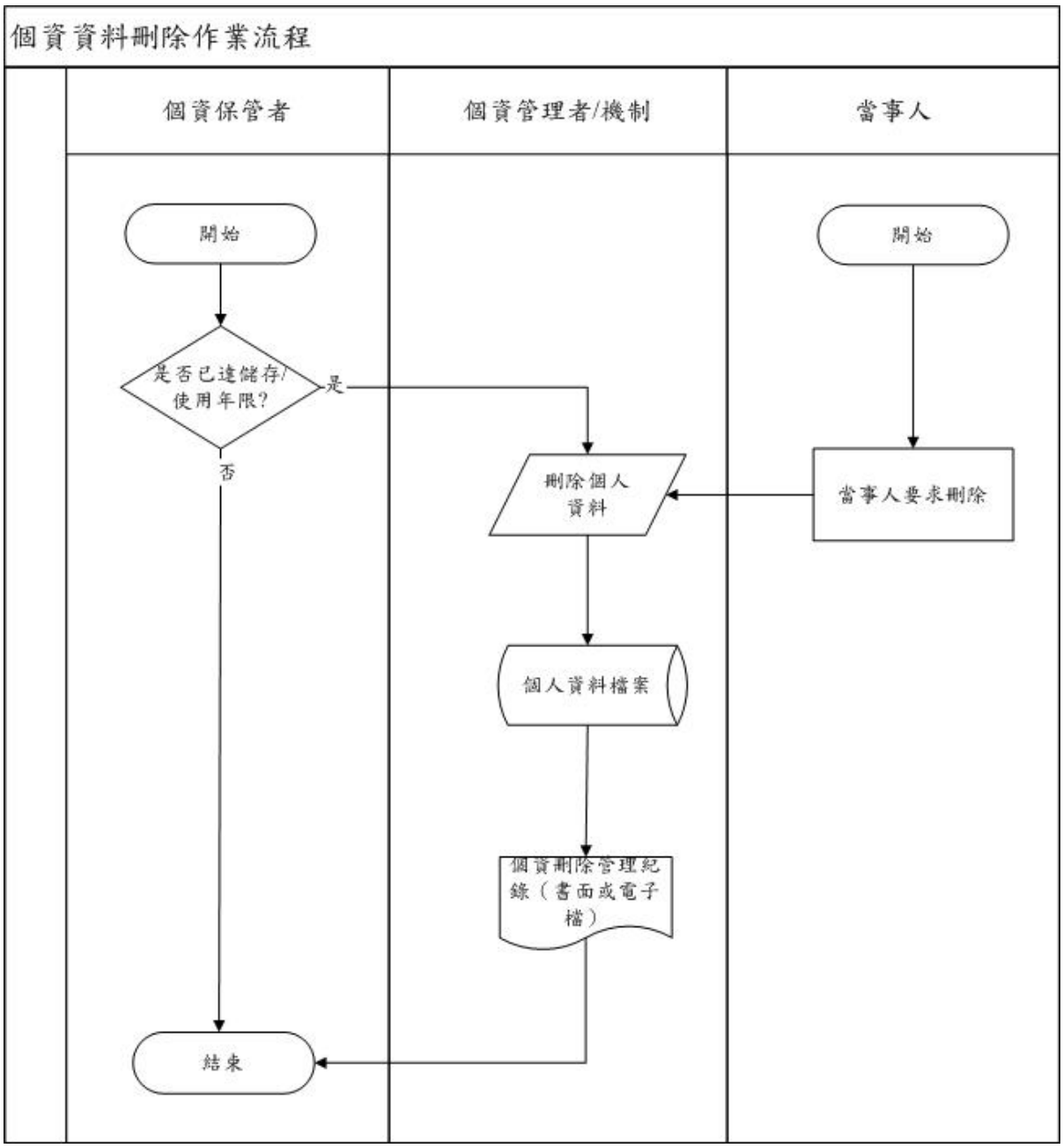
資料來源： 本計畫整理

圖14 個資處理作業流程範例



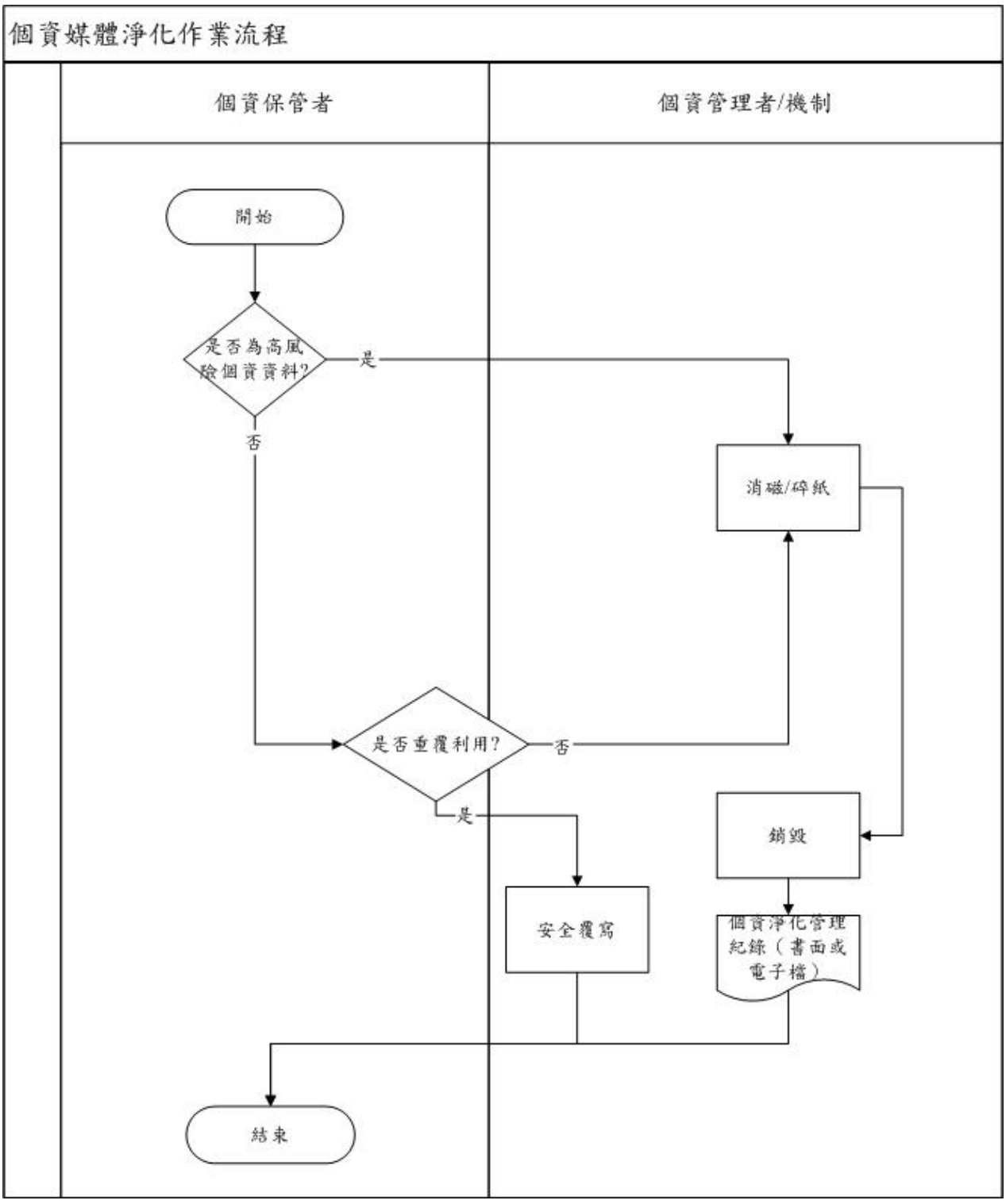
資料來源： 本計畫整理

圖15 個資傳輸作業流程範例



資料來源： 本計畫整理

圖16 個資刪除作業流程範例



資料來源： 本計畫整理

圖17 個資淨化作業流程範例

組織若需於網站或網頁中蒐集個資，應於網站中載明隱私權政策，詳見表20；於蒐集個資時，應請個資擁有者簽署個資提供同意書，詳見表21，明確告知蒐集個資的目的與用途；同時保有個資擁有者需異動與調閱之權利，包括個資補充、資料更正、製給複製本、停止蒐集、處理或利用及資料刪除等時機之用途，詳見表22與表23。

表20 隱私權政策範例(適用於網站)

隱私權政策範例

最後更新日期：xxx 年 xx 月 xx 日

個人資料的蒐集

OO 機關(以下簡稱「本機關」)根據本網站所提供下列服務，將蒐集個人資料：

1、資安教育訓練

2、資安系列競賽

3、資安推廣活動

本機關蒐集的資料如下：

1、真實姓名、身分證字號、職稱、地址、電話、E-mail 電子郵件。

2、我們也蒐集一些不代表您個人，但與您個人相關之訊息，例如您一次瀏覽本網站的頁數，以及伺服器自行產生的相關紀錄，如您使用連線設備的 IP 位置、使用時間、使用的瀏覽器、瀏覽與點選資料紀錄等。本網站會對於個別連線者的瀏覽器予以標示，除非您願意告知您的個人資料，否則在此情況下本網站不會將此項紀錄和您對應。

個人資料的選擇

當您申請需要註冊的特定服務時，我們會要求您提供個人資料。如果此資訊的使用方式與當初蒐集的目的不同，我們會在使用前先徵求您的同意。

如果個人資料的使用用途與本【隱私權政策】或特定服務的隱私權通知所述不同，我們將提供有效的方法，讓您選擇不將個人資料用於這些用途。除非已事先徵得您的同意，否則我們不會蒐集敏感資訊或將之用於與本【隱私權政策】和/或增補服務隱私權通知未涉及之目的。

您可以拒絕向本機關提供個人資料，不過我們可能因此無法為您提供這些服務。

資訊的使用

本網站只有在下列情形下，會向其他機關或個人分享個人資料：

1、已事先徵得您的同意，分享任何機密的個人資料前，我們都會先徵求您的同意。

2、內部分析與研究用途：我們會使用您的資料做為內部統計分析與研究報告用途。

3、委外業務：我們將您的資料提供予負責執行[資安教育訓練]業務且與本機關簽訂委外合約之委外廠商，本機關在合約中要求委外廠商僅可在為本機關執行服務、且無關自身利益的情形下使用您的資料，並遵守本【隱私權政策】和其他適用的任何保密和安全措施。

4、法律要求：本機關於必要時將遵循中華民國法律、命令、傳票、裁判、判斷及處分要求的內容，提供適當的資訊予法定機構，這有可能包括您的個人資料。

5、組織調整：如果本機關因應組織改造所進行之組織調整，我們將確保對涉及這些調整的所有個人資料保密，並在個人資料移轉且被另一隱私權政策約束之前通知您。

Cookies

Cookies 是伺服端為了區別使用者的不同喜好，由瀏覽器寫入使用者硬碟的一些簡短資訊，雖然 Cookies 會識別使用者的電腦，但是無法識別使用者的身分。您也可以透過在您的瀏覽器中選擇修改您對於 Cookies 的接受程度，如果您選擇拒絕所有的 Cookies，您可能無法正常使用部分個人化服務，或是完成[活動或訓練報名業務]。

為了提供更好、更個人化的服務以及方便您參與個人化的互動活動，Cookies 會在您註冊或登入時建立，並在您登出時修改其狀態。

共用資料政策

除本政策的規定外，本網站不會任意出售、交換或出租任何您的個人資料予其他團體或個人。

但是本網站可能為了提供您其他服務或優惠權益(例如[資安推廣之抽獎活動])需要與提供該服務或優惠之第三者共用您的資料，本機關與第三者共用您的個人資料時，本網站將於活動網頁加註資料共用對象說明。

傳送商業或電子郵件之政策

本網站將在事前或註冊登錄取得您的同意後，傳送商業性或電子郵件給您。本網站除了在該資料或電子郵件上註明是由本網站發送，也會在該資料或電子郵件上提供您能隨時停止接收這項服務。或提供您其他服務或優惠權，需要與提供該服務或優惠的第三者傳送商業性資料或電子郵件時，我們將會在活動時提供充分的說明，並且在第三者傳輸之前通知您，您可以自由選擇是否接受這項特定服務或活動。

資訊安全

我們會採取適當的安全措施，來防止未經授權的資料存取、竄改、披露或損毀，其中包括就資料的蒐集、儲存、處理慣例及安全措施進行內部審查，並以實體的安全措施，防止我們儲存個人資料的系統遭到未經授權的存取。

我們只允許本機關的員工和提供特定服務之委外廠商存取個人資料，因為他們需要這些資訊來提供、開發或改善我們的服務。上述人員都必須遵守保密義務，否則可能會遭到懲戒，包括解僱和刑事起訴等。

資料正確性

本機關處理您的個人資料時，會嚴格遵守當初蒐集資訊的目的以及本【隱私權政策】或任何適用的特定服務隱私權通知。我們會審查我們的資料蒐集、儲存及處理慣例，

以確保僅蒐集、儲存及處理提供或改善我們的服務所需的個人資料。我們會採取合理的措施來確保所處理之個人資料的正確性、完整性及即時性，但我們仰賴使用者在必要時更新或修正其個人資料。

查閱和更新個人資料

當您使用本機關服務時，我們會儘量讓您有權查閱自己的個人資料，並讓您修正不正確的資訊，或依您的要求，將法律並未規定需要保留或依合法商業用途不需保留的資料刪除。處理此類要求之前，我們會要求個別使用者證明身分，並指明要查閱、修正或移除的資訊，我們可能會拒絕處理過度重複、經常性、需要過多技術支援、危害其他使用者隱私權、 非常不切實際(例如，索取儲存於備份磁帶上的資訊)或是根本不必要的查閱要求。除非需要大量的技術支援，否則我們會免費讓使用者查閱和修正自己的個人資料。我們有部分服務採用不同的程序來查閱、修正或刪除使用者個人資料。如需這些程序的詳細資訊，請參閱此等服務的特定隱私權通知或常見問題。

自我保護措施

請妥善保管您的任何個人資料，不要將任何個人資料提供給任何人或其他機構。在您使用完本網站所提供的各項服務功能後，務必記得登出，若您是與他人共享電腦或使用公共電腦，切記要關閉瀏覽器視窗，以防止他人讀取您的個人資料或信件。

本政策之修正

由於社會環境及法令規定變遷或科技技術進步，本網站將採用最新技術與法規以盡全力保護您的網路隱私，並且定期審查本網站是否遵守本【隱私權政策】，故本網站有權不定時修訂與公布本【隱私權政策】以合時宜。

為保障您的權益，我們不會在未經您同意的情況下，削減本【隱私權政策】賦予您的權利，即使有變更，多半也只是小幅修正。無論如何，我們會將【隱私權政策】的所有變更都公布在此網頁上，如果是重大變更，我們將提供更明確的通知(某些服務甚至會以電子郵件通知【隱私權政策】的變更)。

本【隱私權政策】的每個版本都會在網頁上方標示生效日期，我們也會將本【隱私權政策】的存檔版本封存，供您檢閱。也請您隨時上網參閱本項聲明。

隱私權保護政策諮詢

如果您有任何本【隱私權政策】或其他關於隱私權管理或本機關使用個人資料的問題，請與我們聯絡，本機關個人資料保護聯絡窗口資訊如下：

個人資料保護服務專線 ：_____

傳真專線電話 ：_____

諮詢服務時間 ：_____

若上述回覆或處理方式無法滿足需求或有任何訴怨內容，請連繫本中心使用者訴怨電子信箱：_____

資料來源： 本計畫整理

表21 個資提供同意書範例

個人資料提供同意書範例

為保障您的權益，請於申請接受 OO 機關（以下簡稱「本機關」）所提供之_____服務(以下簡稱「本服務」)前，詳細閱讀本同意書所有內容。

當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。若您未滿二十歲，應於您的法定代理人閱讀、瞭解並同意本同意書之所有內容及其後修改變更規定後，方得使用本服務，但若您已接受本服務，視為您已取得法定代理人之同意。，並遵守以下所有規範。

一、基本資料之蒐集、更新及保管

1、 本機關蒐集您的個人資料在中華民國個人資料保護法與相關法令之規範下，依據本機關【隱私權政策】，蒐集、處理及利用您的個人資料。

2、 請於申請時提供您本人正確、最新及完整的個人資料。

3、 本機關因執行業務所需蒐集您的個人資料包括姓名、出生年月日、國民身分證統一編號、連絡方式（包括但不限於電話號碼、E-MAIL 或居住地址）及 OOOOO。

4、 若您的個人資料有任何異動，請主動向本機關申請更正，使其保持正確、最新及完整。

5、 若您提供錯誤、不實、過時或不完整或具誤導性的資料，本機關保留隨時終止您接受使用_____服務資格的權利。

6、 您可依中華民國個人資料保護法，就您的個人資料行使以下權利：

(1)請求查詢或閱覽

(2)製給複製本

(3)請求補充或更正

(4)請求停止蒐集、處理及利用

(5)請求刪除

但因本機關執行職務或業務所必須者，本機關得拒絕之。若您欲執行上述權利時，請參考本機關【隱私權政策】之個人資料保護聯絡窗口聯絡方式與本機關連繫。

二、蒐集個人資料之目的

1、 本機關為執行以下業務需蒐集您的個人資料：

(1)資安教育訓練

(2)資安系列競賽

(3)資安推廣活動

2、 當您的個人資料使用方式與當初本機關蒐集的目的不同時，我們會在使用前先徵求您的書面同意，您可以拒絕向本機關提供個人資料，不過我們可能因

此無法為您提供服務。

3、 命資料利用對象為本機關、本機關簽訂委外合約之委外廠商_____及主管機關_____，個人資料處理方式包括個人資料之蒐集、建立、傳送、轉變、儲存、封存與銷毀等資料生週期。資料使用範圍僅限中華民國境內（包括臺澎金馬地區），本機關_____利用您的個人資料期間為永久使用，委外廠商_____利用您的個人資料期間預設為2年，若委外廠商_____因業務需要需延長個人資料使用期間，我們將遵循前項原則，本機關會先徵求您的書面同意後始延長資料使用期限。

三、基本資料之保密

1、 您的個人資料受到本機關【隱私權政策】之保護及規範。請閱讀【隱私權政策】以查閱本機關完整隱私權保護政策。

四、同意書之效力

1、 當您勾選「我同意」並簽署本同意書時，即表示您已閱讀、瞭解並同意本同意書之所有內容，您如違反下列條款時，本機關得隨時終止對您提供之一切服務。

2、 本機關保留隨時修改本同意書規範之權利，本機關將於修改規範時，將於本機關網頁公告修改之事實，不另作個別通知。如果您不同意修改的內容，請勿繼續接受本服務。否則將視為您已同意並接受本規範該等增訂或修改內容之拘束。

3、 您在接受本機關提供的_____服務之前，應仔細閱讀本同意書條款。如您不同意本同意書條款或其更新之內容，您可以放棄接受本機關提供的服務；您一旦接受本同意書，即視為您已瞭解並完全同意本同意書各項條款內容。

4、 您自本同意書取得的任何建議或資訊，無論是書面或口頭形式，除非本同意書條款有明確規定，均不構成本同意書條款以外之任何保證。

九、準據法與管轄法院

1、 本同意書之解釋與適用，以及與本同意書有關的爭議，均應依照中華民國法律予以處理，並以臺灣臺北地方法院為第一審管轄法院。

□ 我已閱讀並且接受上述同意書內容

當事人簽名_____(請親簽)

年　　月　　日

資料來源： 本計畫整理

表22 個人資料異動申請書範例

<table>
<tr><td rowspan="2">申請人姓名
(請檢附證件)</td><td></td><td>申請人簽名</td><td>(請親簽)</td></tr>
<tr><td>£當事人 £代理人(與當事人關係_____)</td><td>承辦人</td><td>承辦人姓名_____
核對身分確認，£本人 £非本人</td></tr>
<tr><td>申請目的
(請勾選一項)</td><td colspan="3">£資料補充 £資料更正 £製給複製本 £停止蒐集、處理或利用 £資料刪除
原因(請詳述)：_____
_____</td></tr>
<tr><td>檔案名稱</td><td colspan="3"></td></tr>
<tr><td>資料項目
(請勾選)</td><td>£當事人所有個資
£姓名
£身分證字號</td><td>£出生年月日
£戶籍地址
£通訊方式</td><td>£_____
£_____
£_____</td></tr>
<tr><td>資料說明</td><td colspan="3"></td></tr>
<tr><td colspan="4">以下由 OO 機關人員填寫</td></tr>
<tr><td>資訊型態</td><td colspan="3">£紙本，名稱_____ £電子檔，檔名_____
£資料庫，名稱_____ £其他：_____</td></tr>
<tr><td>處理方式</td><td colspan="3"></td></tr>
<tr><td colspan="2">保管人</td><td>科長</td><td>主管</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

資料來源： 本計畫整理

表23 個資調閱申請書範例

<table>
<tr><td rowspan="2">申請人姓名
(請檢附證件)</td><td colspan="4"></td></tr>
<tr><td colspan="2">£當事人 £代理人(與當事人關係_____)</td><td>連絡電話</td><td></td></tr>
<tr><td>調閱目的
(請詳述)</td><td colspan="4"></td></tr>
<tr><td>資訊型態</td><td colspan="4">£紙本 £電子檔(PDF) £電子檔(DOC) £電子檔(PPT)
£電子檔(XLS) £電子檔(其他：_____) £其他：_____</td></tr>
<tr><td>調閱對象</td><td colspan="4">姓名(個人)：_____；範圍(非特定對象)：_____</td></tr>
<tr><td>調閱項目
(請勾選)</td><td>£身分證字號
£姓名
£出生年月日</td><td>£通訊電話
£通訊住址
£戶籍地址</td><td colspan="2">£_____
£_____
£_____</td></tr>
<tr><td colspan="2">保管人</td><td>科長</td><td colspan="2">主管</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">說明：
1、 資料申請者為組織單位時，不得做為個人使用。
2、資料申請者同意對於個資的運用與保密，如有違反「個人資料保護法」之相關規定者，悉依該法第五章之相關罰則辦理。</td></tr>
</table>

資料來源： 本計畫整理

Ÿ 設計個資事故管理作業流程

於現行資安事故通報應變程序與流程中，檢視並調整作業程序，以符合個資法之相關要求。有關資安事故通報與紀錄表範例，請參考附件 7。

組織若尚未訂定事故管理程序，可參考國家資通安全通報應變網站之「資

安事件通報應變機制說明」，訂定個資事故通報應變處理程序。

Ÿ 設計個資管理稽核作業流程

依照個資作業流程、作業程序書(蒐集、處理及傳輸)及事故通報與作業程序文件，訂定個資內部稽核作業程序，或於現行稽核作業程序中，檢討調整個資檢核項目，至少一年需執行一次稽核作業。有關稽核計畫、查核表及紀錄，請參考附件 8、附件 9 及附件 10。

Ÿ 修訂組織內部管理制度文件

依據個資作業流程，檢視並綜整組織內部管理制度文件，同時重新發布更新版之管理制度文件。

3.2.3. 建立安全控制措施

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。

建立安全控制措施之任務，包括分析個資保護技術安全控制項目基準值需求、規劃個資生命週期保護構面控制項目行動方案、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、規劃基礎設施網路安全管理構面控制項目行動方案，以及建置個資保護安全控制項目行動方案。有關每項任務內容，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，另外，為確保技術性防護措施。已經審慎評估考量，可參照「個資管理防護架構」(詳見圖 10)，檢視個資技術

性防禦之完整性。

實際作法可參照「個資保護技術安全控制項目基準值」建議 (詳見表 17)，使用「個資項目技術安全控制措施基準值評估表」(詳見附件 11)，檢核個資項目技術性安全控制措施；若個資資料為紙本，則僅需檢視編號內含「＊」符號之項目即可。例如，若個資項目對應之技術控制措施等級為「中」， 即可參考「個資項目技術控制措施基準值評估表」，進行個資安全保護技術控制措施基準值符合度評估，詳見表 24。

表24 個資項目技術安全控制措施基準值評估表範例

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
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	

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
					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機關之外部連線外，亦包括使用者於本機關非使用本機登入，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)連線至本機關資訊系統之存取活動
17				中	本機關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機關資訊系統之活動，均符合本機關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
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

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
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，若連接至本機關內部網路與資訊系統時，是否已經過授權始可使用	可攜式行動裝置包括外接儲存設備(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，若連接至本機關內部網路與資訊系統時，是否符合本機關資訊安全原則	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機關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機關之可攜式裝置(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、是否額外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
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	若事件稽核日誌包括敏感/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	

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
					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	重大變更包括資訊資產、組態項目、資產、人員或組織形態有重大變更，或是個資法條文有異動
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）						
46				普	使用者帳號是否具有唯一鑑識性	使用者包括本機關正職員工、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括使用者帳號、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(包括透過 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
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	

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
					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(包括電子郵件)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	資訊系統媒體包括電子媒體(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括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
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	本控制項應包括資訊系統媒體(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	本控制項應包括資訊系統媒體、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

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
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	
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)方式包括媒體清除(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機關內部人員使用；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	
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機關之資訊系統

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
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，應用程式包括 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	
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，內部包括系統監視、內部網路或系統元件之間的事件偵測工具，外部則包括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	

No	Checkbox			Level	Control	Note
	Yes	**No**	**N/A**			
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	檢測項目至少包括 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

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。

3.2.4. 個資委外作業管理

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。

個資委外作業管理之任務，包括檢視個資委外作業契約與範圍、調整個資委外作業合約與工作計畫書內容、規劃個資委外作業稽核計畫及執行個資委外作業稽核。有關每項任務內容，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，詳見附件 12。

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，詳見附件 13；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，詳見表 25 與表 26。

表25 委外合約個資保護條款範例

OO 委外合約

甲方：OO 機關

乙方：OOOOOOO

合約條款...

隱私保護：

- 乙方僅得為辦理本合約所載委外業務之相關目的，蒐集、處理、利用或傳輸_____個人資料，並應符合個人資料保護法、其他相關法規命令及甲方所訂定之個資保護相關規範，個資保護活動應依據甲方執行個資衝擊分析與個資風險評估結果等級所對應之個資管理流程與個資保護措施辦理之。乙方若有違反，致_____個人資料遭不法蒐集、處理、利用或其他侵害者，乙方應負賠償責任。
- 甲方得保留對乙方實施個資管理稽核之權利，以確認乙方是否落實相關個資管理作業。
- 乙方參與本合約專案成員，皆應簽署「保密切結書」。

資料來源： 本計畫整理

表26 保密切結書個資保護條款範例

保 密 切 結 書

立書人：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

茲因立書人受ＯＯ機關委託執行＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿專案/業務，立書人同意就執行專案/業務過程中接觸之機密資訊與/或個人資料，願負保密義務如下：

一、本切結書所稱個人資料」，係指ＯＯ機關交付立書人或立書人因接受ＯＯ機關委託執行專案/業務所需蒐集由「個人資料保護法」所定義，包括但不限於姓名、身分證字號、通訊資料等之個人資料。

二、 保密義務

1. 立書人應採取與自己處理或保管機密資訊與/或個人資料之相同標準(但不得低於合理之標準)，保管ＯＯ機關所揭露之機密資訊與/或個人資料，且僅得為執行專案/業務之目的而使用機密資訊與/或個人資料。未經ＯＯ機關事前書面同意，不得以任何方式直接或間接交付或洩漏機密資訊予第三人，且不得為自己或第三人之利益使用機密資訊與/或個人資料。

2. 立書人應負責使其員工與其履行輔助人遵守本切結書之保密義務，且不因離職而終止。

3. 立書人因進行，必須將機密資訊與/或個人資料揭露予第三人時，應事前取得本機關之書面同意及該第三人對於機密資訊與/或個人資料保密之書面承諾，立書人並就該第三人承諾負連帶履行之義務。

4. 立書人因法院或主管機關之命令，須揭露機密資訊與/或個人資料時，應於收到命令後立即通知ＯＯ機關，並配合ＯＯ機關採取合理必要之保密措施。

5. 立書人願遵守「個人資料保護法」之相關法令，於執行ＯＯ機關之專案/業務時，不得私自蒐集與本專案/業務無關之任何個人資料。

6. 立書人應依據「個人資料保護法」之規範，對相關個人資料保護盡善良管理人之義務。

三、立書人如發現第三人未經授權或違法使用機密資訊與/或個人資料，應立即通知本機關，並配合採取必要之排除或防止措施。

四、立書人如違反本切結書之各項義務時，ＯＯ機關除得隨時要求返還或銷毀機密資訊與/或個人資料及其所有之重製物外，立書人並應賠償本機關因此所生之一切損害(包括但不限於訴訟費與律師費)。

資料來源： 本計畫整理

3.2.5. 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。

宣導與教育訓練之任務，包括規劃個資認知宣導活動、規劃個資管理認知與教育訓練計畫及執行個資管理認知與教育訓練計畫。有關每項任務內容，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(詳見附件 14)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。

組織可依據認知、一般及專業 3 大類別，建立人員年度個資管理認知與訓練計畫表，包括各類人員年度最低學習學分時數要求。

- 認知類

內容著重在建立人員對個資管理的基本認知，以及相關法規命令說明，適合所有同仁參與，新進同仁須在一年內完成個資管理的基礎認知課程。

- 一般類

內容著重在訓練人員瞭解個資管理應有的流程與技術控制措施作業方式，適合所有同仁參與，上課同仁應先完成個資管理基礎認知課程。

- 專業類

內容著重在培養個資管理專責人員，瞭解並熟悉個資防護系統相關活動之執行方式，與技術控制措施有關之應用系統或工具之操作與管理。

3.3.檢查

檢查階段之重要工作為維護個資管理系統，透過管理檢視、稽核活動及管理審查活動之進行，檢測管理品質之有效性，持續提升個資防護整體成效。

本階段之活動，包括個資管理報告檢視、個資管理稽核活動及個資事故追蹤處理，有關本階段之輸入項目、產出項目及執行手法與相關工具，詳見表 27，分述如下：

表27 檢查階段活動與任務表

活動與任務(Activity & Task)	輸入項目(Input)	產出項目(Output)	執行方法與相關工具(Technique & Tool)
Activity1：個資管理報告檢視			
Task1：彙整前一檢視週期個資事故紀錄	前一檢視週期個資事故通報與處理紀錄	個資事故通報與處理紀錄彙整	資料蒐集與分析、小組會議
Task2：彙整前一檢視週期個資流程管理紀錄	前一檢視週期相關個資生命週期作業流程管理紀錄	個資生命週期作業流程管理紀錄彙整	資料蒐集與分析、小組會議、相關作業程序書
Task3：彙整前一檢視週期個資保護安全控制項目管理紀錄	前一檢視週期相關個資保護安全控制項目管理紀錄	個資保護安全控制項目管理紀錄彙整	資料蒐集與分析、小組會議、個資保護安全控制項目基準值建議表
Task4：彙整前一檢視週期個資管理認知與教育訓練計畫執行紀錄	前一檢視週期個資管理訓練計畫執行紀錄	個資管理訓練計畫執行紀錄彙整	資料蒐集與分析、小組會議、年度個資管理認知與訓練計畫
Task5：進行個資管理預期目標與實值之差異分析	個人資料保護管理要點與相關作業目標、各項彙整紀錄	個資管理目標差異分析項目	資料蒐集與分析、小組會議、預防與矯正行動方案範例

活動與任務(Activity & Task)	輸入項目(Input)	產出項目(Output)	執行方法與相關工具 (Technique & Tool)
Task6：研擬差異項目之預防與矯正行動方案建議	個資管理目標差異分析項目	個資管理預防與矯正行動方案	資料蒐集與分析、小組會議、預防與矯正行動方案範例
Activity2：個資管理稽核活動			
Task1：安排個資管理內部稽核人員與職責分工	個資管理組織架構圖、作業流程或管理制度程序書		個資管理組織架構圖
Task2：規劃個資管理內部稽核計畫	個人資料保護管理要點、個資作業程序書		稽核計畫範例
Task3：核可與通知個資管理內部稽核計畫		個資管理內部稽核計畫	管理會議
Task4：執行個資管理內部稽核	個資管理內部稽核計畫	個資管理內部稽核紀錄	個資管理紀錄蒐集、實地稽核、稽核紀錄表範例
Task5：完成個資管理內部稽核報告	個資管理內部稽核紀錄	個資管理內部稽核報告	資料分析、稽核報告範例
Task6：研擬預防與矯正行動方案	個資管理內部稽核報告	預防與矯正行動方案	預防與矯正行動方案範例

活動與任務(Activity & Task)	輸入項目(Input)	產出項目(Output)	執行方法與相關工具(Technique & Tool)
建議			
Activity3：個資事故追蹤處理			
Task1：個資事故識別與登錄	個資事故	個資事故通報與紀錄表	個資事故通報與紀錄表範例
Task2：進行個資事故範圍控制與調查	個資事故通報與紀錄表	個資事故通報與紀錄表	資料蒐集與分析、小組會議、個資事故通報與紀錄表範例
Task3：進行個資事故通報	資安(個資)事故通報作業程序、個資事故通報與紀錄表	資安(個資)事故通報紀錄、個資事故通報與紀錄表	資料蒐集與分析、個資事故通報與紀錄表範例
Task4：擬定個資管理新增控制措施建議	個資事故通報與紀錄表	個資事故通報與紀錄表、個資管理預防與矯正行動方案	資料蒐集與分析、小組會議、預防與矯正行動方案範例
Task5：完成個資事故結案	個資事故通報與紀錄表	個資事故通報與紀錄表	個資事故通報與紀錄表範例、管理會議

資料來源： 本計畫整理

3.3.1. 個資管理報告檢視

為掌握個資管理情形，應定期檢視個資管理相關報告，確保目前的管控狀況符合個資管理政策與目標，如未達管理目標，應適時提出改善計畫，以維護個資管理品質。

個資管理報告檢視之任務，包括彙整前一檢視週期個資事故紀錄、彙整前一檢視週期個資流程管理紀錄、彙整前一檢視週期個資保護安全控制項目管理紀錄、彙整前一檢視週期個資管理認知、教育訓練計畫執行紀錄、進行個資管理預期目標與實值之差異分析及研擬差異項目之預防與矯正行動方案建議。有關每項任務內容，說明如下：

Ÿ 彙整前一檢視週期個資事故紀錄

個資事故紀錄應定期檢視，視需要召開會議，分析個資事故之樣態與趨勢，確保相關通報與應變措施順利執行。

Ÿ 彙整前一檢視週期個資流程管理紀錄

有關個資生命週期所涉及之管理措施，包括個資蒐集、處理、利用及傳輸於組織內部訂定之程序書，應定期檢視其管理紀錄，瞭解目前實施之安全控制項目是否能達成個資保護之目標。

Ÿ 彙整前一檢視週期個資保護安全控制項目管理紀錄

定期檢視個資保護安全控制項目之管理紀錄，本項措施可結合前項措施一同執行，確保管理程序與安全控制互相搭配，且符合目前之安全防護趨勢與要求。

Ÿ 彙整前一檢視週期個資管理認知與教育訓練計畫執行紀錄

依照個資管理認知與教育訓練計畫，定期檢視實際執行成效，並針對教育

訓練出席率較低之情形，執行補強措施。

Ÿ 進行個資管理預期目標與實值之差異分析

彙整以上四項個資管理措施紀錄，分析是否符合預期目標，並做其差異分析，瞭解未能達成目標之原因。

Ÿ 研擬差異項目之預防與矯正行動方案建議

依照差異分析結果，研擬預防與矯正行動方案，請參考附件 15；並依照行動方案內容，提供適當之人力、物力及財力等相關資源。

3.3.2. 個資管理稽核活動

定期執行個資管理稽核活動，有助於瞭解各項管控措施是否已落實執行，以利於管理審查會議時一併追蹤檢討。

個資管理稽核活動之任務，包括安排個資管理內部稽核人員與職責分工、規劃個資管理內部稽核計畫、核可與通知個資管理內部稽核計畫、執行個資管理內部稽核、完成個資管理內部稽核報告及研擬預防與矯正行動方案建議。有關每項任務內容，說明如下：

Ÿ 安排個資管理內部稽核人員與職責分工

依照內部稽核管理程序，執行個資內稽作業，遴選參與人員，並做細部職責分工，選定主導稽核員與稽核員，同時可培育觀察員一同參與。本項稽核活動可結合管理制度之稽核活動，共同辦理。

Ÿ 規劃個資管理內部稽核計畫

研擬個資管理內部稽核計畫，規劃稽核範圍、方法、時程及依據，包括個資法、組織內個資作業要點、政策及個資推動之各項作業程序。有關稽核計畫、查核表及紀錄範例，請參考附件 8、附件 9 及附件 10。

- 核可與通知個資管理內部稽核計畫

  由管理階層核可內部稽核計畫，並通知內部人員配合稽核行程，參與稽核活動。

- 執行個資管理內部稽核

  依稽核計畫訂定之內部稽核時程，執行個資管理內部稽核，蒐集與記錄個資管理資料。

- 完成個資管理內部稽核報告

  將個資管理內部稽核之檢視紀錄，彙整成個資管理內部稽核報告。

- 研擬預防與矯正行動方案建議

  針對內部稽核報告中發現之不符合事項或重大缺失，應擬定預防與矯正行動方案建議，以有效解決問題，提升個資防護效能。

3.3.3. 個資事故追蹤處理

因應個資事故通報與處理回應，包括對於個資事故所需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，並與組織相關資安事故程序整合運作，以發揮流程運作之效率。

將個資安全事故管理流程和現行 ISO/IEC 20000 與 CNS/ISO/IEC 27001 之事故管理，整合為一致之事故管理流程，對於重大個資事故應進行事後檢視，並提出合適的預防行動方案。對於個資事故的管理，平時就應讓同仁充分瞭解何謂個資外洩相關事故，以及在事故發生時，需要彙報的資訊以減少個資外洩可能造成的損失。例如以下資訊：

- 事故由誰彙報。
- 事故由誰發現。

- 事故發生/發現之日期及時間。
- 事故的本質。
- 發生事故的系統以及相關聯之其他系統。
- 已損失或受危及的資料內容。
- 儲存已損失或受危及資料之硬體設施。
- 避免未經授權之使用已損失或受危及資料控制。
- 潛在可能受影響之個人。
- 是否已通報警檢單位。

個資事故追蹤處理之任務，包括個資事故識別與登錄、進行個資事故範圍控制與調查、進行個資事故通報、擬定個資管理新增控制措施建議及完成個資事故結案。有關每項任務內容，說明如下：

- 個資事故識別與登錄

  在發生事故時，鑑別是否為個資事故，確認為個資事故後，依組織訂定之個資事故通報應變流程，填寫個資事故通報與紀錄表單。

- 進行個資事故通報

  於填寫個資事故通報與紀錄表後，進行個資事故通報作業，本項作業可與前項措施同步進行。

- 進行個資事故範圍控制與調查

  針對個資事故內容，進行資料蒐集與分析，包括數位證據的彙整，同時瞭解發生原因與行為模式，調查個資事故影響情形與影響範圍，並處理事故。

- 擬定個資管理新增控制措施建議

當個資事故無法即時解決，或該事故一再重複發生時，即應擬定適當的保護措施，透過增加管理或技術控制措施，以加強個資防護強度，有效防制問題發生。

Ÿ 完成個資事故結案

更新個資事故通報與紀錄表，填寫處理作為，並經核定後結案。

3.4.行動

行動階段之重要工作為管理組織審查會議及個資管理改善計畫，有關本階段之輸入項目、產出項目及執行手法與相關工具，詳見表 28，分述如下：

表28 行動階段活動與任務表

活動與任務(Activity & Task)	輸入項目(Input)	產出項目(Output)	執行方法與相關工具(Technique & Tool)
Activity1：管理組織審查會議			
Task1：彙整外部最新個資相關法規命令	個資法、個資法施行細則、個資法相關法規命令	管理審查會議會議資料	資料蒐集與分析、小組會議
Task2：彙整個資管理預防與矯正行動方案	個資管理預防與矯正行動方案	管理審查會議會議資料	資料蒐集與分析、小組會議
Task3：彙整個資事故追蹤處理結果	個資事故通報與紀錄表、個資管理預防與矯正行動方案	管理審查會議會議資料	資料蒐集與分析、小組會議
Task4：彙整內部與個資委外作業稽核結果	個資管理內部稽核報告、個資委外作業稽核紀錄	管理審查會議會議資料	資料蒐集與分析、小組會議
Task5：舉行管理組織審查會議	管理審查會議議程、管理審查會議會議資料	管理審查會議會議紀錄、個資管理改善計畫	管理審查會議作業流程
Activity2：個資管理改善計畫			
Task1：安排個資管理改善計畫相	個資管理改善計畫		小組會議、研討會、

活動與任務(Activity & Task)	輸入項目(Input)	產出項目(Output)	執行方法與相關工具(Technique & Tool)
關人力與資源			管理會議
Task2：執行個資管理改善計畫		執行結果紀錄	資料蒐集與分析、小組會議
Task3：檢視個資管理改善計畫執行結果	執行結果紀錄	個資管理改善計畫執行結果檢視紀錄	資料蒐集與分析、小組會議

資料來源： 本計畫整理

3.4.1. 管理組織審查會議

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。

管理組織審查會議之任務，包括彙整外部最新個資相關法規命令、彙整個資管理預防與矯正行動方案、彙整個資事故追蹤處理結果、彙整內部與個資委外作業稽核結果及舉行管理組織審查會議。有關每項任務內容，說明如下：

- 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。

- 彙整個資管理預防與矯正行動方案

  本項內容包括 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。

3.4.2. 個資管理改善計畫

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。

個資管理改善計畫之任務，包括安排個資管理改善計畫相關人力與資源、執行個資管理改善計畫及檢視個資管理改善計畫執行結果。有關每項任務內容，說明如下：

- 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。

- 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。

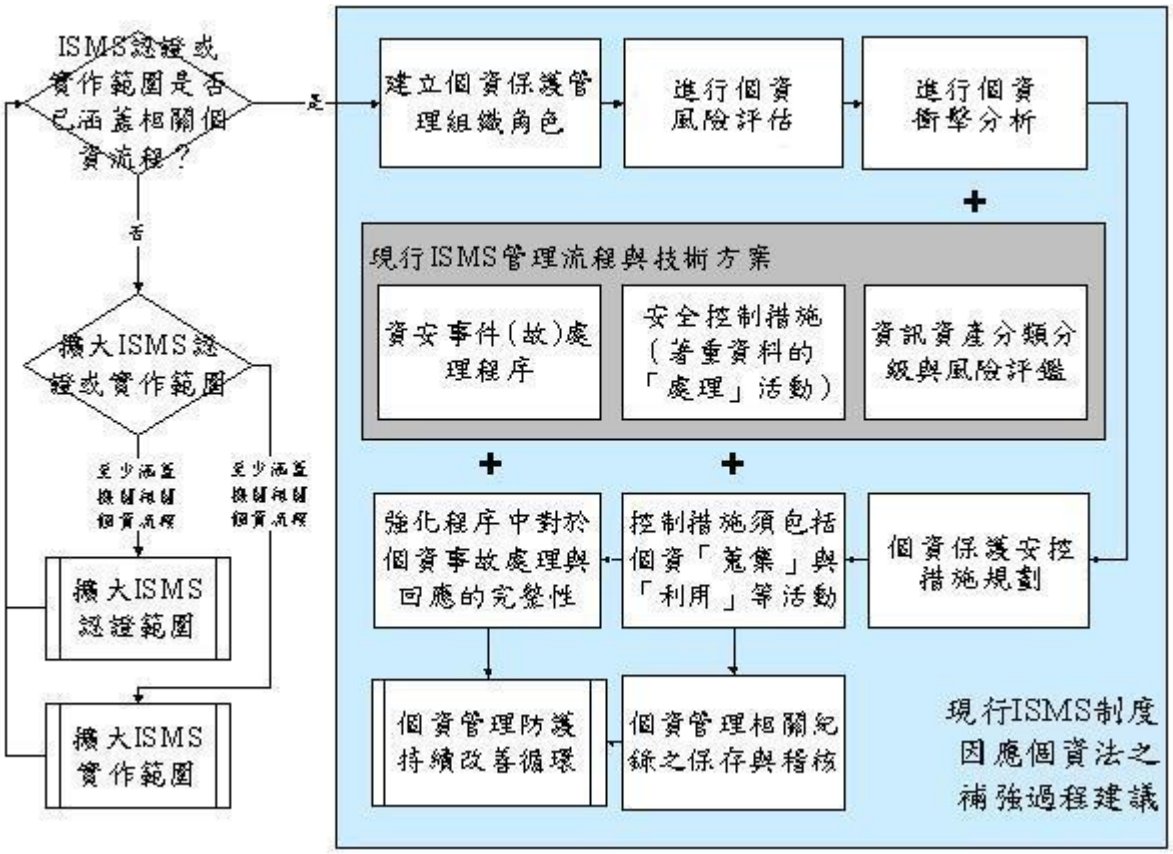
- 檢視個資管理改善計畫執行結果

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。

3.5.資訊安全管理制度(ISMS)與個資保護導入

由於政府推動資訊安全管理系統政策已有多年，對於已通過 CNS/ISO/IEC 27001 驗證的組織而言，如何在既有的資訊安全管理制度基礎，達到制度整合且發揮管理綜效，是必須考量的重要課題，組織進行個資管理與資訊安全管理系統之整合建議流程，詳見圖 18。



資料來源： 本計畫整理

圖18 個資管理與資訊安全管理系統之整合建議

基於法規命令要求，組織必須將個資全面性納入管理，因此若組織現行之 ISMS 驗證範圍未涵蓋全組織，建議可先將現行 ISMS 驗證範圍擴大，以涵蓋組織相關個資流程。接著再建立個資保護管理組織，此外，可將 ISMS

中與個資有關之類別(如為文件與資訊等)，依據個資屬性新增對應的次分類，例如加入包括一般個資或特種個資內容的文件或資訊類別，同時在 ISMS 的風險評鑑與風險處理等項目中，建議可加入與個資相關之弱點/威脅評估及個資保護技術性安全控制，即可整合 ISMS 與個資項目之風險評鑑作業，以利於組織採一致化的風險評鑑產出結果，進行風險處理對策之研擬與行動方案之規劃。

對於個資管理行動方案的實作，不論是管理制度或技術控制措施，必須注意通常 ISMS 的管控較著重在個資實際的處理流程上，但從個資法的角度與規範要求，對於個資的蒐集或利用等活動的管理也同樣重要，因此在既有的 ISMS 安全控制措施基礎上，必須補強個資項目在其他相關生命週期活動中的安全控制措施需求。有關個資蒐集、處理或利用等活動的流程管理制度與技術控制措施實作建議，請參見 3.2.2 建立個資管理程序與 3.1.9 安全控制措施規劃。

為因應個資事故通報與後續處理回應之實務需要，與對於個資事故之數位證據與數位鑑識處理上的需求，建議可整合個資事故通報流程，於原有的資安事故通報程序中，增加下列項目：

- 個資事故負責通報人員。
- 個資事故發現者。
- 個資事故發生與發現之日期與時間。
- 個資事故性質與敘述。
- 個資事故影響範圍(包括系統、人員及組織) 。
- 遭受揭露之個資範圍與敘述。
- 遭受揭露個資之儲存媒體。

- 個資事故相關採證程序之紀錄、證據保存方式及負責人員。
- 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) 。
- 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。
- 個資事故可能影響之當事人範圍與人數。
- 通知個資事故當事人之通報對象、內容、方式及時機。
- 內部調查結果說明。

對於尚未通過 CNS/ISO/IEC 27001 驗證的組織而言，藉由個資保護管理建置流程進行個資管理，可為組織建立部分資訊安全管理制度的應用基礎，未來當組織開始導入資訊安全管理系統時，亦方便組織將已建立的個資管理程序與活動整合其中。

同時參考 CNS/ISO/IEC 27001 之建置流程步驟內容，將各步驟所對應之個資管理主要活動整理列表詳見表 29。

表29 CNS/ISO/IEC 27001 建置流程步驟對應之個資管理主要活動

CNS/ISO/IEC 27001 建置流程步驟	相關個人資料管理主要活動
1.獲得管理階層支持	1.獲得管理階層支持
2.定義 ISMS 適用範圍	2.建立個人資料保護要點與隱私政策
3.盤點資訊資產	3.盤點個人資料檔案
4a.定義風險評鑑方法	4a.定義個資衝擊分析與衝擊評鑑方法
4b.執行資訊安全風險評鑑	4b.執行個人資料檔案之個資衝擊分析與衝擊評鑑

CNS/ISO/IEC 27001 建置流程步驟	相關個人資料管理主要活動
5a.準備適用性聲明書	5a.進行個資管理整體準備度評估
5b.準備風險處理計畫	5b.準備個資流程管理與安全控制措施建置計畫
6.發展 ISMS 建置計畫	6.規劃個資流程管理與安全控制措施
7.執行 ISMS 建置計畫	7.執行個資流程管理與安全控制措施建置計畫
8.完成 ISMS 建置計畫	8.完成個資流程管理與安全控制措施建置計畫
9.ISMS 活動產出	9.個資管理活動與紀錄保存
10.遵循性檢視	10.個資法與相關施行細則遵循性檢視
11.矯正行動	11.個資事故回應與矯正行動
12.預評	12.個資管理內部稽核
13.驗證稽核	13.個資委外作業稽核
14.通過驗證	14.管理審查會議

資料來源： http://www.iso27001security.com/html/27001.html，本計畫整理

4. 個資保護管理建置實務

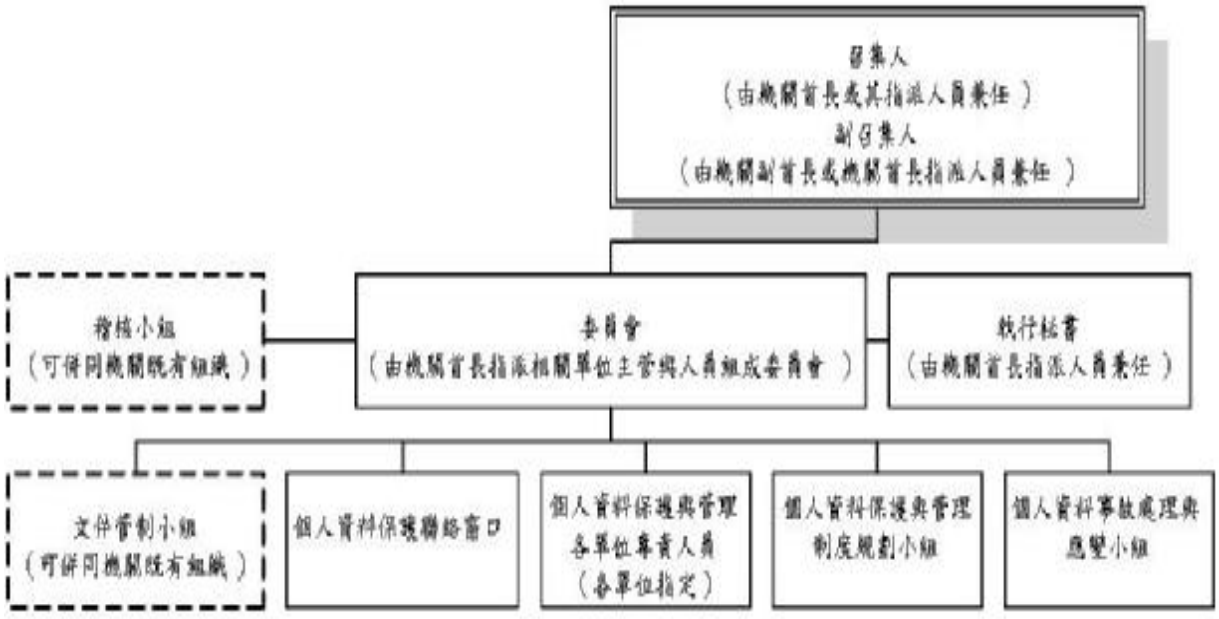
本章將透過情境範例，引導政府機關依據個資保護管理建置流程，逐步建立機關之個資保護管理制度。

情境範例說明：

由於個資法於 101 年 10 月 1 日正式施行，施行細則法務部亦已頒布， A 機關為瞭解機關內所擁有個資項目、可能面臨的衝擊及因應作法，因此，導入個資保護管理制度，以符合個資法之要求。

4.1.建立個資保護管理組織

首先，於導入個資保護管理制度前，先於機關內實施全面性之個資管理認知課程，機關亦於教育訓練後，成立個人資料保護管理組織(組織架構詳見圖 19)，正式推動個資保護管理。



資料來源： 本計畫整理

圖19 A 機關個人資料保護管理組織架構

組織中各角色職責分述如下：

Ÿ 召集人

由機關首長或其指派人員兼任，主要職責包括：

– 機關個人資料保護與管理機制的最高負責人。

– 審核並頒行機關的個人資料保護與隱私政策。

– 提供建立與維運個人資料管理機制所需的資源。

– 核定個人資料管理文件的制訂、修訂及廢止。

– 指派個人資料管理組織架構相關角色人員，包括：

Ø 執行秘書及其代理人。

Ø 個人資料保護管理委員會委員。

Ø 個人資料保護聯絡窗口。

Ø 稽核小組、文件管制小組、個人資料保護與管理制度規劃小組、個人資料事故處理與應變小組之組長。

– 核可各單位提報之個人資料保護與管理專責人員。

– 擔任機關個人資料保護與管理審查會議之主持人。

– 核可個人資料保護與管理內部稽核之稽核計畫與稽核報告

Ÿ 副召集人

由機關副首長或機關首長指派人員兼任，主要職責為協助召集人辦理個人資料保護相關事宜，並為召集人之代理人。

Ÿ 執行秘書

由召集人指派人員兼任，主要職責包括：

– 協助召集人推行個人資料保護與管理。

– 傳達召集人之決策，以貫徹個人資料保護與管理。

– 依召集人指示，執行個人資料保護與管理機制之變更作業。

– 負責統籌與協調各小組相關個人資料保護作業之運作。

– 將個人資料保護管理委員會與各小組對重大事宜之建議、意見、資料及報告，彙集、轉陳予召集人進行決策。

– 定期蒐集、分析及陳報個人資料保護與管理相關通報及處理狀況報告。

– 協助追蹤、管理個人資料保護與管理稽核作業所提相關建議事項。

Ÿ 個人資料保護管理委員會

由召集人指派相關單位主管與人員組成委員會，主要職責包括：

– 個人資料保護與管理機制適法性與合宜性之檢視、審議及評估。

– 個人資料保護與管理相關辦法內容之諮詢、討論及決議。

– 指派各單位個人資料保護與管理專責人員。

– 記錄個人資料保護管理委員會之會議紀錄。

– 指導個人資料保護與管理各小組與專責人員之作業。

– 審核個人資料保護與管理內部稽核之稽核計畫與稽核報告。

– 審核個人資料保護與管理內部人員認知與教育訓練計畫。

– 審核個人資料保護與管理技術控制與基礎設施之提升計畫。

Ÿ 個人資料保護聯絡窗口

由召集人指派人員擔任，主要職責包括：

– 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。

Ÿ 各單位個人資料保護與管理專責人員

由各單位提報，經召集人核可後擔任，主要職責包括：

– 接受個人資料保護管理委員會、執行祕書、個人資料保護管理組織各小組之指導，落實相關個人資料保護與管理活動之推動。

– 協助各單位人員進行個人資料保護與管理活動。

– 呈報各單位個人資料保護與管理推動之狀況予執行祕書或個人資料保護管理組織相關小組。

– 通報各單位個人資料事故，協助進行相關個人資料事故應變及處理。

– 處理當事人依法提出個人資料權利之請求事宜。

Ÿ 個人資料保護與管理制度規劃小組

由召集人指派人員擔任小組組長，小組成員由組長陳報召集人核可後組成，主要職責包括：

– 依據個人資料保護法、施行細則等相關法規命令對機關之影響，提出適法性之因應措施與計畫。

– 研擬個人資料保護與管理相關辦法、程序、細則及表單內容。

– 研擬個人資料保護與管理相關委外作業合約與監督辦法內容。

– 研擬個人資料保護與管理內部人員認知與教育訓練計畫。

– 研擬個人資料保護與管理技術控制與基礎設施之提升計畫。

– 研擬以 PDCA（Plan-Do-Check-Act）方法，持續提升個人資料保護與管理機制之運作，包括個人資料檔案之維護、隱私衝擊與風險分析、安全維護措施基準值之持續評估等。

Ÿ 個人資料事故處理與應變小組

由召集人指派人員擔任小組組長，小組成員由組長陳報召集人核可後組成，主要職責包括：

– 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。

Ÿ 稽核小組

同機關內部既有之稽核組織，並於原有職責中納入對個人資料保護與管理之相關稽核作業要求。

Ÿ 文件管制小組

同機關內部既有之文件管制組織，並於原有管理範圍中納入個人資料保護與管理機制相關政策、程序文件、作業細則、應用表單、個人資料檔案及軌跡資料檔。

4.2.個資項目盤點

經個資保護管理組織決議，就資訊單位所擁有的機關網站中之資料與系統，檢視應納入個資保護管理的範圍，並指派個人資料保護與管理制度規劃小組組長負責導入全般事宜。

案經規劃小組組長主導，由資訊單位承辦人依個資流程分析表進行檢視後，該承辦人共彙整出「機關網站中會員註冊與單一登入」、「帳號申請」、「Web 應用服務，及其它 E 化服務」及「以 DB 帳號直接登入 DB 存取個資」等 4 項流程具有「個資會員註冊資料(直接蒐集) 」、「帳號申請資料(初次申請) 」、「帳號申請資料(異動) 」、「查詢人資料」、「申請人資料 (Web 應用服務)管理者異動申請表」、「會員註冊資料(間接蒐集) 」、「Web 應用服務查詢結果」、「申請人資料 (Web 應用服務)管理者異動申請表」、「會員資料存取軌跡資料-OMLOG(使用者) 」、「會員資料存取軌跡資料-OS LOG(管理者) 」、「Web 應用服務 Query Result 之軌跡資料--OS LOG」、「Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG」、「Web 應用服務查詢人之軌跡資料-OS LOG」及「以 DB 帳號直接登入 DB 存取個資之存取軌跡資料」等 14 項個資檔案，應納入個資保護管理。

經規劃小組組長採人員訪談方式，訪談資訊單位承辦人與委外廠商，先蒐集資料以瞭解該單位各作業流程或應用系統中可能留存之個資範圍，再就個資蒐集範圍填註個資項目基本資料。繼由資訊單位承辦人與委外廠商，就個資管理相關活動與各個資項目利害關係人，填註個資項目生命週期與個資項目利害關係人表，綜整前述相關資料完成個資項目盤點。個資項目蒐集範圍、個資項目基本資料、個資項目生命週期、個資項目利害關係人及個資項目盤點表等各項範例詳見表 30、表 31、表 32、表 33 及表 34。

表30 機關網站個資項目蒐集範圍範例

業務或服務作業流程			個人資料檔案基本資訊	個人資料欄位																						間接識別的欄位
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	Y	Y	Y														Y					
2	機關網站	帳號申請	帳號申請資料(異動)	Y	Y	Y				Y	Y									Y					
3	機關網站	帳號申請	帳號申請資料(初次申請)	Y	Y	Y				Y	Y									Y					
4	機關網站	Web 應用服務，及其它 E 化服務	查詢人資料																						
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	Y		Y														Y					
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	Y	Y	Y							Y							Y					
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	Y	Y	Y				Y	Y		Y							Y	Y				
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表			Y														Y					
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)																					Y	存取人代號,存取時間,執行的動作

業務或服務作業流程			個人資料檔案基本資訊	個人資料欄位																					間接識別的欄位
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)																					Y	存取人代號,存取時間,執行的動作,ip
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)																					Y	存取人代號,存取時間,執行的動作
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG(使用者無法存取,此項僅針對管理者)																					Y	存取人代號,存取時間,執行的動作
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)																					Y	存取人代號,存取時間,執行的動作

業務或服務作業流程			個人資料檔案基本資訊	個人資料欄位																					間接識別的欄位
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	
14	機關網站	以 DB 帳號直接登入 DB 存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以 DB 帳號直接登入 DB 存取個資之存取軌跡資料																					Y	

資料來源： 本計畫整理

表31 機關網站個資項目基本資料範例

業務或服務作業流程			個人資料檔案基本資訊					
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	資訊單位	數位檔		065	C001, C011, C038, C052
2	機關網站	帳號申請	帳號申請資料(異動)	資訊單位	影像檔		002	C001, C003
3	機關網站	帳號申請	帳號申請資料(初次申請)	資訊單位	影像檔		002	C001, C003
4	機關網站	Web 應用服務，及其它 E 化服務	查詢人資料	資訊單位	數位檔		065	C001, C003
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	資訊單位	實體紙本		065	C001, C003, C011
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	資訊單位	數位檔		065	C001, C011, C038, C052
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	資訊單位	數位檔		065	C001, C011, C038, C021
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	資訊單位	數位檔		065	C001, C003, C011
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	資訊單位	數位檔		065	C001
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	資訊單位	數位檔		065	C001

業務或服務作業流程			個人資料檔案基本資訊					
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001
14	機關網站	以DB帳號直接登入DB存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以DB帳號直接登入DB存取個資之存取軌跡資料	資訊單位	數位檔		065	C001

資料來源： 本計畫整理

表32 機關網站個資項目生命週期範例

業務或服務作業流程			個人資料檔案名稱	個人資料檔案生命週期活動									
編號	服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或備異地援位置	法定保存期限	自訂保存期限	內部連結或對傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	直接	維運團隊(申請者自行線上打)	機關網站	機房-機關網站資料庫	備份機房	N/A	持續使用之帳號永久保存；另將調整「5年間未使用帳號予以刪除」	與網站進行單一登入介接之系統；應用程式與應用程式間傳輸	刪除DB資料	N/A
2	機關網站	帳號申請	帳號申請資料(異動)	直接	客服團隊	傳真(主)/email 客服(少量)	客服團隊留存於mail server/fax server	主機備份於同大樓，由IT部門管理人控管	N/A	永久保存；email為12個月(合約規範)	客服團隊將申請資料email轉派由維運團隊處理	N/A	N/A
3	機關網站	帳號申請	帳號申請資料(初次申請)	直接	客服團隊	傳真(主)/email 客服(少量)	客服團隊留存於mail server/fax server	主機備份於同大樓，由IT部門管理人控管	N/A	永久保存(自訂)；email為12個月(合約規範)	N/A	N/A	N/A
4	機關網	Web應用服務，及其它E化服務	查詢人資料	直接	維運團隊(系統	機關網站(Web應用服務)	機房-機關網站資料庫	備份機房	N/A	已排定計畫刪除	N/A	刪除DB資料	N/A

業務或服務作業流程			個人資料檔案名稱	個人資料檔案生命週期活動									
編號	服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	內部連結或傳送對象與方式	刪除銷毀方式	國際傳輸對象與方式
	站				自動存記)								
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	直接	維運團隊	傳真至機關承辦人(後續由機關轉送維運團隊)	機關網站維運團隊之上鎖檔案櫃	N/A	N/A	重要稽核紀錄，永久保存	N/A	碎紙銷毀	N/A
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	間接	維運團隊	其他部會系統	機房-機關網站資料庫	備份機房	N/A	持續使用之帳號永久保存；另將調整「5 年間未使用帳號予以刪除」	與網站進行單一登入介接之系統；應用程式與應用程式間傳輸	刪除 DB 資料	N/A
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	間接	維運團隊	FTP、HTTP(依 Web 應用服務提供機關需求，於系統暫存查詢結果資料，以供使用者自行下載查詢結果)	機房-機關網站資料庫	備份機房	N/A	3 個月 (依 Web 應用服務提供機關需求，以系統排程自動刪除)	經 Web 應用服務提供機關授權可透過本服務查調資料的公務機關人員	刪除 DB 資料	N/A
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	直接	維運團隊	服務人員電腦	服務人員電腦	N/A	N/A	重要稽核紀錄，永久保存	N/A	刪除信件	N/A

業務或服務作業流程			個人資料檔案名稱	個人資料檔案生命週期活動									
編號	服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	內部連結或傳送對象與方式	刪除銷毀方式	國際傳輸對象與方式
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	間接	維運團隊	系統收集	機房-機關網站資料庫	備份機房	N/A	永久保存	N/A	N/A	N/A
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	間接	維運團隊	系統收集	機房-機關網站資料庫	備份機房	N/A	永久保存	N/A	N/A	N/A
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	間接	維運團隊	系統收集	機房-機關網站資料庫	備份機房	N/A	5 年 3 個月	N/A	刪除 DB 資料	N/A
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG(使用者無法存取,此項僅針對管理者)	間接	維運團隊	系統收集	機房-機關網站資料庫	備份機房	N/A	永久保存	N/A	N/A	N/A
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料 -OS LOG(使用者無法存取,此項僅針對管理者)	間接	維運團隊	系統收集	機房-機關網站資料庫	備份機房	N/A	永久保存	N/A	N/A	N/A

業務或服務作業流程			個人資料檔案名稱	個人資料檔案生命週期活動									
編號	服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	內部與連結或傳送對象方式	刪除銷毀方式	國際傳輸對象與方式
14	機關網站	以 DB 帳號直接登入 DB 存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以 DB 帳號直接登入 DB 存取個資之存取軌跡資料	間接		系統收集	機房 - 機關網站資料庫	備份機房	N/A	永久保存	N/A	永久保存	N/A

資料來源： 本計畫整理

表33 機關網站個資項目利害關係人表範例

業務或服務作業流程			個人資料檔案名稱	利害關係人				
編號	服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	民眾、公務員	資訊處	維運團隊	無	SSO 介接之系統相關人員
2	機關網站	帳號申請	帳號申請資料(異動)	公務員	資訊處	客服團隊、維運團隊	無	
3	機關網站	帳號申請	帳號申請資料(初次申請)	公務員	資訊處	客服團隊	無	無
4	機關網站	Web 應用服務，及其它 E 化服務	查詢人資料	公務員	資訊處	維運團隊	無	Web 應用服務提供之機關
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	公務員	資訊處	維運團隊	無	無
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	民眾、公務員	資訊處	維運團隊	無	SSO 介接之系統相關人員
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	民眾、公務員	資訊處	維運團隊	無	無
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	公務員	資訊處	維運團隊	無	無
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	民眾、公務員	資訊處	維運團隊	無	無
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	維運團隊	資訊處	維運團隊	無	無

業務或服務作業流程			個人資料檔案名稱	利害關係人				
編號	服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	公務員	資訊處	維運團隊	無	無
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG(使用者無法存取,此項僅針對管理者)	維運團隊	資訊處	維運團隊	無	無
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料 -OS LOG(使用者無法存取,此項僅針對管理者)	民眾	資訊處	維運團隊	無	無
14	機關網站	以 DB 帳號直接登入 DB 存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以 DB 帳號直接登入 DB 存取個資之存取軌跡資料	維運團隊	資訊處	維運團隊	無	無

資料來源： 本計畫整理

表34 機關網站個資項目盤點表範例

業務或服務作業流程			個人資料檔案基本資訊						利害關係人				
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	資訊單位	數位檔		065	C001, C011, C038, C052	民眾、公務員	資訊處	維運團隊	無	SSO 介接之系統相關人員
2	機關網站	帳號申請	帳號申請資料(異動)	資訊單位	影像檔		002	C001, C003	公務員	資訊處	客服團隊、維運團隊	無	
3	機關網站	帳號申請	帳號申請資料(初次申請)	資訊單位	影像檔		002	C001, C003	公務員	資訊處	客服團隊	無	無
4	機關網站	Web 應用服務，及其它E化服務	查詢人資料	資訊單位	數位檔		065	C001, C003	公務員	資訊處	維運團隊	無	Web 應用服務提供之機關
5	機關網站	Web 應用服務，及其它E化服務	申請人資料(Web 應用服務)管理者異動申請表	資訊單位	實體紙本		065	C001, C003, C011	公務員	資訊處	維運團隊	無	無
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	資訊單位	數位檔		065	C001, C011, C038, C052	民眾、公務員	資訊處	維運團隊	無	SSO 介接之系統相關人員
7	機關網站	Web 應用服務，及其它E化服務	Web 應用服務查詢結果	資訊單位	數位檔		065	C001, C011, C038, C021	民眾、公務員	資訊處	維運團隊	無	無
8	機關網站	Web 應用服務，及其它E化服務	申請人資料(Web 應用服務)管理者異動申請表	資訊單位	數位檔		065	C001, C003, C011	公務員	資訊處	維運團隊	無	無
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	資訊單位	數位檔		065	C001	民眾、公務員	資訊處	維運團隊	無	無

業務或服務作業流程			個人資料檔案基本資訊						利害關係人				
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	資訊單位	數位檔		065	C001	維運團隊	資訊處	維運團隊	無	無
11	機關網站	Web 應用服務，及其它E化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001	公務員	資訊處	維運團隊	無	無
12	機關網站	Web 應用服務，及其它E化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001	維運團隊	資訊處	維運團隊	無	無
13	機關網站	Web 應用服務，及其它E化服務	Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)	資訊單位	數位檔		065	C001	民眾	資訊處	維運團隊	無	無

業務或服務作業流程			個人資料檔案基本資訊						利害關係人				
編號	服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
14	機關網站	以DB帳號直接登入DB存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以DB帳號直接登入DB存取個資之存取軌跡資料	資訊單位	數位檔		065	C001	維運團隊	資訊處	維運團隊	無	無

資料來源： 本計畫整理

4.3.個資項目衝擊分析與個資項目衝擊評鑑

搭配先前完成之個資項目盤點，由規劃小組組長採人員訪談方式與所蒐集之資料，訪談資訊單位承辦人與委外廠商，填註個資項目衝擊分析表，共同完成個資項目之個資衝擊分析範例詳見表 35。

次就個資項目衝擊分析所得，檢討各個資項目依個資風險等級基準值所列含有個資類別、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，評估各層面風險等級，綜整各層面風險等級採最高原則方式評定各個資項目個資性之風險等級範例詳見表 36。

表35 個資項目衝擊分析表範例

業務或服務作業流程			個人資料檔案名稱	隱私衝擊分析																
編號	服務目錄或流程名稱	子流程名稱		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
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	>50,000	5,000-50,000	5-10	部份	N/A	持續使用之帳號永久保存；另將調整「5 年間未使用帳號予以刪除」	是	否	0.無確認	否		是	是	是	部份	是	是	否
2	機關網站	帳號申請	帳號申請資料(異動)	5,000-50,000	500-5,000	5-10	是	N/A	永久保存；email 為 12 個月(合約規範)	是	否	2.書面核對相關證明文件	否		是	是	部份	不適用	否	是	是
3	機關網站	帳號申請	帳號申請資料(初次申請)	5,000-50,000	500-5,000	5-10	是	N/A	永久保存 (自訂)；email 為 12 個月(合約規範)	是	否	2.書面核對相關證明文件	否		是	是	部份	不適用	否	是	是
4	機關網站	Web 應用服務，及其它 E 化服務	查詢人資料	1-500	1-500	1-5	部份	N/A	已排定計畫刪除	是	否	2.書面核對相關證明文件	否		是	是	是	是	否	否	否
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料(Web 應用服務)管理者異動申請表	1-500	1-500	1-5	部份	N/A	重要稽核紀錄，永久保存	是	否	2.書面核對相關證明文件	否		是	是	是	是	否	是	否
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	>50,000	5,000-50,000	5-10	否	N/A	持續使用之帳號永久保存；另將調整「5 年間未使用帳號予以刪除」	是	否	3.與其他來源進行交叉比對	否		是	是	部份	部份	是	是	否

業務或服務作業流程			個人資料檔案名稱	隱私衝擊分析																
編號	服務目錄或流程名稱	子流程名稱		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
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	>50,000	>50,000	5-10	不適用	N/A	3 個月 (依 Web 應用服務提供機關需求,以系統排程自動刪除)	是	否	3.與其他來源進行交叉比對	否		否	否	否	否	否	否	否
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料(Web 應用服務)管理者異動申請表	1-500	1-500	1-5	部份	N/A	重要稽核紀錄，永久保存	是	否	2.書面核對相關證明文件	否		是	是	是	是	否	否	否
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	>50,000	>50,000	1-5	不適用	N/A	永久保存	是	否	0.無確認	否		不適用	不適用	否	否	否	否	否
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	>50,000	>50,000	1-5	不適用	N/A	永久保存	是	否	0.無確認	否		不適用	不適用	否	否	否	否	否
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	>50,000	>50,000	1-5	不適用	N/A	5 年 3 個月	是	否	0.無確認	否		不適用	不適用	否	否	否	否	否

業務或服務作業流程			個人資料檔案名稱	隱私衝擊分析																
編號	服務目錄或流程名稱	子流程名稱		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
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG(使用者無法存取,此項僅針對管理者)	>50,000	>50,000	1-5	不適用	N/A	永久保存	是	否	0.無確認	否		不適用	不適用	否	否	否	否	否
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)	>50,000	>50,000	1-6	不適用	N/A	永久保存	是	否	0.無確認	否		不適用	不適用	否	否	否	否	否
14	機關網站	以 DB 帳號直接登入 DB 存取個資(DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以 DB 帳號直接登入 DB 存取個資之存取軌跡資料	>50,000	>50,000		不適用	N/A	永久保存	是	否	0.無確認	否		否	否	否	否	否	否	否

業務或服務作業流程			個人資料檔案名稱	隱私衝擊分析																	
編號	服務目錄或流程名稱	子流程名稱		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

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：每筆資料中包括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

表36 個資項目衝擊評鑑範例

業務或服務作業流程			個人資料檔案名稱	PIA/RA 安全控制項目基準值			個資性之風險等級
編號	服務目錄或流程名稱	子流程名稱		含有個資類別	NIST SP800-122 之衝擊等級判定方式	「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	
1	機關網站	會員註冊與單一登入	會員註冊資料(直接蒐集)	高	中	高	高
2	機關網站	帳號申請	帳號申請資料(異動)	高	中	中	高
3	機關網站	帳號申請	帳號申請資料(初次申請)	高	中	中	高
4	機關網站	Web 應用服務，及其它 E 化服務	查詢人資料	普	普	普	普
5	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	普	普	普	普
6	機關網站	會員註冊與單一登入	會員註冊資料(間接蒐集)	高	中	高	高
7	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢結果	高	中	高	高
8	機關網站	Web 應用服務，及其它 E 化服務	申請人資料 (Web 應用服務)管理者異動申請表	普	普	普	普

業務或服務作業流程			個人資料檔案名稱	PIA/RA 安全控制項目基準值			個資性之風險等級
編號	服務目錄或流程名稱	子流程名稱		含有個資類別	NIST SP800-122之衝擊等級判定方式	「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	
9	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OMLOG(使用者)	普	普	普	普
10	機關網站	會員註冊與單一登入	會員資料存取軌跡資料-OS LOG(管理者)	普	普	普	普
11	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	普	普	普	普
12	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS LOG(使用者無法存取,此項僅針對管理者)	普	普	普	普
13	機關網站	Web 應用服務，及其它 E 化服務	Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)	普	普	普	普

業務或服務作業流程			個人資料檔案名稱	PIA/RA 安全控制項目基準值			個資性之風險等級
編號	服務目錄或流程名稱	子流程名稱		含有個資類別	NIST SP800-122 之衝擊等級判定方式	「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	
14	機關網站	以 DB 帳號直接登入 DB 存取個資 (DBA、程式開發者) -因「維護/程式開發/臨時性產出資料」等非經由線上程式之存取	以 DB 帳號直接登入 DB 存取個資之存取軌跡資料	普	普	普	普

資料來源： 本計畫整理

4.4.個資人員權責角色訂定

該機關網站之人員權限，依照平台之個人資料檔案，填寫「個資項目與個資管理角色對應表」詳見表 37。

4.5.個資安控措施評估

以服務目錄或流程名稱為「機關網站」，其中之個人資料檔案名稱為「會員註冊資料」為例，設若個資項目對應之技術控制措施等級為「高」， 使用「個資項目技術控制措施基準值評估表」(詳見附件 10)，進行個資安全保護技術控制措施基準值符合度評估，範例詳見表 38。

表37 個資項目與個資管理角色對應表範例

勾選說明：**R**有權限**T**無權限

個資管理角色 / 個人資料檔案	計畫承辦窗口							計畫承辦窗口主管							委外廠商窗口							委外廠商窗口主管						
	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出
會員註冊資料(直接蒐集)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
帳號申請資料(異動)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
帳號申請資料(初次申請)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
查詢人資料	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
申請人資料(Web 應用服務)管理者異動申請表	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
會員註冊資料(間接蒐集)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**

個資管理角色 / 個人資料檔案	計畫承辦窗口							計畫承辦窗口主管							委外廠商窗口							委外廠商窗口主管						
	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出
Web 應用服務查詢結果	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
申請人資料(Web 應用服務)管理者異動申請表	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
會員資料存取軌跡資料-OMLOG(使用者)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
會員資料存取軌跡資料-OS LOG(管理者)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
Web 應用服務 Query Result 之軌跡資料--OS LOG(使用者無法存取,此項僅針對管理者)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
Web 應用服務管理者異動申請表之軌跡資料--個人電腦之 OS	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**

個資管理角色 / 個人資料檔案	計畫承辦窗口							計畫承辦窗口主管							委外廠商窗口							委外廠商窗口主管						
	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出
LOG(使用者無法存取,此項僅針對管理者)																												
Web 應用服務查詢人之軌跡資料-OS LOG(使用者無法存取,此項僅針對管理者)	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**
以 DB 帳號直接登入 DB 存取個資之存取軌跡資料	**T**	**T**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**T**	**T**	**T**	**T**	**T**	**T**	**T**

資料來源： 本計畫整理

表38 個資項目技術安全控制措施基準值評估表範例

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
技術控制措施類別：(1)存取控制機制							
1	V			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	V			普	是否已建立應用層之存取控制		使用帳號管理辦法
3	V			普	是否已依據密碼原則設定密碼		資通安全政策
4	V			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	電腦資源管理辦法
5	V			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	電腦資源管理辦法
6	V			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；	資訊處理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						或採用以角色為基礎的存取控制機制	
7		V		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		V		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		V		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	
技術控制措施類別：(2)職務區隔							

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
10	V			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)	工作計畫書
11	V			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	工作計畫書
12	V			中	執行存取控制者是否禁止稽核自身相關工作		內部資訊安全稽核程序
13	V			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 個部份交由 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	系統管理員均有不同帳號及使用 EAP
14	V			高	Level 等級中之內容是否完全		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					符合		
技術控制措施類別：(3)最小權限							
15	V			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	V			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機關之外部連線外，亦包括使用者於本機關非使用本機登入，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)連線至本機關資訊系統之存取活動	電腦資源管理辦法
17	V			中	本機關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機關資訊系統之活動均符合本機關所訂定之	主機及伺服器管理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						遠端存取政策	
18	V			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	使用專線線路
19	V			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		使用 IPSec
20	V			高	Level 等級中之內容是否完全		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					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	V			中	是否已禁止將個資儲存於共享資料夾		伺服器上線服務主機資安查核表
22	V			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	使用者帳號管理辦法
23			V	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	V			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	密碼已使用 hash
25	V			高	Level 等級中之內容是否完全符合		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
26	V			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	密碼已使用 hash
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	V			普	可攜式行動裝置若連接至本機關內部網路與資訊系統時是否已經過授權始可使用	可攜式行動裝置包括外接儲存設備(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/通訊設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等)	電腦資源管理辦法
28	V			普	可攜式行動裝置若連接至本機關內部網路與資訊系統時是否符合本機關資訊安全原則	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	資安稽核項目評核表

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						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	V			普	可攜式行動裝置若連接至本機關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)	資安稽核項目評核表
30			V	普	若人員需要攜出屬於本機關之可攜式裝置(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	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	

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					屬於高風險		
31	V			中	Level 等級普之內容是否完全符合		
32	V			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)		電腦資源管理辦法
33	V			中	是否已禁止使用私有之可攜式媒體		電腦資源管理辦法
34	V			中	是否已禁止無特定保管者之可攜式媒體的使用		電腦資源管理辦法
35		V		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	
36		V		高	Level 等級中之內容是否完全符合		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
技術控制措施類別：(7)稽核事件							
37	V			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)		主機及伺服器管理辦法
38	V			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	主機及伺服器管理辦法
39	V			中	若事件稽核日誌包括敏感/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		客戶資料擷取作業申請表

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
40	V			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		V		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		V		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	重大變更包括資訊資產、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		V		中	Level 等級普之內容是否完全符合		
44		V		高	Level 等級中之內容是否完全符合		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
45	V			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機關相關人員進行調查與回應	主機及伺服器管理辦法
技術控制措施類別：(9)識別與鑑別(機關使用者）							
46	V			普	使用者帳號是否具有唯一鑑識性	使用者包括本機關正職員工、約聘員工、顧問等	使用者帳號管理辦法
47	V			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	使用者帳號管理辦法
48	V			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	使用者身分認證方式包括使用者帳號、密碼、token、生物辨識(如指紋辨識)，機敏性較高之系統亦	使用 EAP 系統

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					多元識別(multifactor authentication)等認證方式	可使用二元識別(two-factor authentication)或多元識別(multifactor authentication)等認證方式	
49	V			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(包括透過LAN、WAN或VPN等方式)		使用者帳號管理辦法
50	V			中	Level 等級普之內容是否完全符合		
51	V			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		系統管理員使用 EAP 系統
52	V			中	資訊系統之最高權限或特殊		系統管理員使用 EAP 系統

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					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	V			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	系統管理員使用 EAP 系統
54	V			高	Level 等級中之內容是否完全符合		
55	V			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		僅遠端登入使用 EAP 系統
56	V			高	所有使用者於遠端登入時，是	如使用含 token 動態密碼之二/多	使用 EAP 系統

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					否已採用重送攻擊防阻之認證機制(replay resistant authentication)	元認證或時間戳記(timestamp)認證協定	
57		V		高	傳送電子文件(包括電子郵件)時是否已使用數位簽章		
技術控制措施類別：(10)媒體存取							
58	V			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	資訊系統媒體包括電子媒體(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)	資訊處理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
59		V		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		V		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	V			中	個資等級標示範圍是否已包括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	資訊處理辦法
62	V			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	
63	V			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	V			中	存放儲存個資儲存媒體之場所是否已設有實體管控措	本控制項應包括資訊系統媒體(相關定義請參考「媒體存取」控制	資訊處理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					施，並限制可接觸該媒體之人員	措施說明)、可攜式行動裝置(相關定義請參考「可攜式行動裝置之存取控制」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		V		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		V		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	V			中	是否已限制負責傳輸或傳送存有個資儲存媒體之人員	本控制項應包括資訊系統媒體、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)	資訊處理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
68	V			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	資訊處理辦法
69	V			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	資訊處理辦法
70	V			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	客戶資料擷取作業申請表附件
71			V	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		
72	V			高	Level 等級中之內容是否完全符合		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
73	V			高	是否已指派專人負責遞送個資儲存媒體		客戶資料擷取作業申請表附件
技術控制措施類別：(14)媒體淨化							
74	V			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)方式包括媒體清除(clear)、刪除(purge)及破壞(destroy) 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	資訊處理辦法、以軟體進行至少 7 次覆寫、實體破壞及消磁

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						‧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	V			中	Level 等級普之內容是否完全符合		
76		V		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機關內部人員使用；將報廢之電子儲存媒體則應採取消磁或實體破壞方式銷毀 ▪ 非電子儲存媒體則應透過水銷	

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						或焚燒方式銷毀	
77		V		高	Level 等級中之內容是否完全符合		
78		V		高	是否已追蹤、記錄並核對儲存媒體淨化與銷毀程序		
79		V		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		V		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機關之資訊系統	
81		V		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		

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					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	V			中	資料傳輸時是否已進行加密，	本控制項適用於透過內外部網路、無線網路之資料傳輸，應用程式包括 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	資訊處理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
						使用 128 位元以上進行加密	
83	V			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	網路及網路設備管理辦法
84	V			高	Level 等級中之內容是否完全符合		
85	V			高	是否已禁止使用無線網路傳輸等級為高之資料		
技術控制措施類別：(16)靜態資訊的保護							
86		V		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	

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
87		V		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	V			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，內部包括系統監視、內部網路或系統元件之間的事件偵測工具，外部則包括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	安裝 IPS、FW、HONEYPOT、WAF、及 LOG SERVER 等防護工具，並進行通報
89	V			中	是否已設置防火牆(firewall)協助進行網路監控與防護		網路及網路設備管理辦法
90	V			中	是否已設置惡意軟體偵測(如		伺服器上線服務主機查核表網路

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					防毒軟體、防木馬間諜軟體等)協助進行網路監控與防護		
91	V			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		安裝 IPS 與 LOG SERVER
92	V			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		SPAM 設備過濾
93	V			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		主機及伺服器管理辦法
94	V			中	資訊系統監視工具是否已架		網路及網路設備管理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					設於本機關與外部網路連接界限、重要伺服器與內部網路界限		
95	V			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	主機及伺服器管理辦法
96	V			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	主機及伺服器管理辦法
97	V			中	自動化監測工具若需自行設定政策、過濾條件(如firewall、MIMESweeper 等)，	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	主機及伺服器管理辦法 網路及網路設備管理辦法

No	Checkbox			Level	Control	Note	現行對應程序文件
	Yes	No	N/A				
					是否已定期檢視相關政策與設定		
98	V			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	主機及伺服器管理辦法
99	V			中	自行開發之系統是否已執行原始碼檢測	檢測項目至少包括 OWASP Top 10 等著名安全風險	將採購硬體執行此功能
100	V			高	Level 等級中之內容是否完全符合		

資料來源： 本計畫整理

4.6.個資委外管理

由於 A 機關的委外處理業務中，有部分與個資相關，因此，規劃小組組長於檢視委外管理相關作業程序與現況後，發現機關於委外專案需求說明書中，與個資相關的規範字樣如下：本機關擁有「依據承包廠商資安政策與個資保護政策」進行「資安稽核」與「個資保護稽核」之權力。為使委外需求說明書中的個資要求更臻於完善，經請教個資保護專家後，建議於委外需求說明書中，加入以下對個人資料保護與管理之標準需求說明：

- 承包廠商應建立隱私保護政策,承包廠商與承包廠商人員應遵循本機關的隱私權政策、個人資料保護與管理辦法、及相關個人資料保護與管理要求,承包廠商與承包廠商人員應對本專案相關個人資料檔案負保護與管理責任，並符合個人資料保護法等相關法規命令要求。
- 承包廠商須提供參與本案人員個人資料保護與管理教育訓練,並舉行測驗,教育訓練內容須包括人員對個人資料保護的認知,個人資料檔案蒐集、處理及利用的作業要求等,教育訓練內容及測驗卷送本機關備查。
- 未經本機關事先書面同意,承包廠商不得將本專案相關個人資料檔案攜出履約地點。若有事先經本機關書面允許之情形,承包廠商應於本專案終止前將相關個人資料檔案交還本機關,同時承包廠商不得對任何交還之個人資料檔案進行複印、複製、攝錄影及拍照等各式保存行為。
- 承包廠商應建立個資事故之正式通報程序及管道,並訂定通報後應採行之處理措施,如相關個人資料遭受侵害時,承包廠商應依事前訂定之通報管道立即通報本機關。
- 本機關於本專案有效期間暨專案合約正式終止後一年內,得不定期至承包廠商場所稽核其對於本專案相關個人資料蒐集、處理及利用情形，以防個人資料外洩或遭受侵害，確保個人資料保護與管理之要求。

4.7.個資宣導與教育訓練

A 機關亦依據認知、一般及專業 3 大類別，建立人員年度個資管理認知與訓練計畫表，包括各類人員年度最低學習學分時數要求。計畫表範例詳見表 39。

表39 年度個資管理認知與訓練計畫表範例

課程類別	課程名稱	學分數	實施頻率	參加對象		
				主管人員	個資管理專責人員	一般同仁
認知	個資管理基礎認知課程	1.5	每年	O	O	O
認知	個資規命令充電課程	1.5	每半年	O	O	O
一般訓練	個資(蒐集)生命週期作業流程說明	1	每年	O	O	O
一般訓練	個資(利用與處理)生命週期作業流程說明	1	每年	O	O	O
一般訓練	個資(蒐集)生命週期技術措施說明	1	每年		視需要	視需要
一般訓練	個資(利用與處理)生命週期技術措施說明	1	每年		視需要	視需要
專業訓練	個資流程與項目盤點實務課程	1	每年		O	
專業訓練	個資衝擊分析實務課程	1	每年		O	
專業訓練	個資風險評估實務課程	1	每年		O	
專業訓練	DLP(XX)技術課程	1	每年		視需要	

資料來源： 本計畫整理

4.8.個資管理審查

為使管理者掌握個資保護管理制度之推動成效，應定期於管理審查會議中，討論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。以下為 A 機關在個資保護管理制度導入過程中，提請於管理審查會議中之審查項目，詳見表 40。

4.9.個資管理改善

本次導入活動，經個資盤點、評鑑、安控措施評估後，提供以下八項建議行動方案，以及與個資法之要求相互對應，以期做為日後改善之執行措施，詳如表 41。

表40 管審會審查項目建議表

管理階層審查項目	建議事項	是/否審查	有/無資料
先前管理階層審查之跟催措施		Y	Y
前次外稽審查報告矯正狀況		Y	Y
資訊安全稽核與審查結果 (含預防與矯正措施之狀況)	增加個資保護管理內部稽核結果、委外廠商個資保護管理稽核結果	Y	Y
風險評鑑報告與風險處理計畫執行狀況(含先前風險評鑑未適切提出之脆弱點或威脅)	增加個人資料檔案之盤點、隱私衝擊分析及風險評估結果，與個資相關安全維護措施改善行動方案的執行狀況	Y	Y
ISMS 與個人資料保護管理文件異動狀態彙總		Y	Y
相關團體之意見回饋	審視個資保護相關法令法規內容之異動影響	Y	Y
改進資訊安全管理系統與個人資料保護管理機制之績效性及有效性之技術、產品或程序方法		Y	Y
有效性評量的結果	當事人依個資法提出請求的項目、內容、數量及回覆處理效率之分析	Y	Y
可能影響資訊安全管理系統與個人資料保護管理機制之任何變更		Y	N

管理階層審查項目	建議事項	是/否審查	有/無資料
改進之建議 & 其它待管審會決議事項		Y	Y
個資事故處理與應變紀錄之審查		Y	Y

資料來源： 本計畫整理

表41 個資行動方案建議表

項次	個資管理程序需求	建議行動方案	個資法相關要求
1	提供當事人行使下列權利時之聯繫窗口與方式： 一、查詢或請求閱覽 二、請求製給複製本 三、請求補充或更正 四、請求停止蒐集、處理或利用 五、請求刪除	1.以機關公開供公眾查閱之保有機關聯絡方式作為當事人的主要聯繫窗口 2.規劃當事人行使相關權利的作業流程並設計相關申請單供當事人使用 3.規劃查詢或請求閱覽個人資料或製給複製本者，得酌收之必要成本費用	第 3 條：當事人權利之行使；第 8 條：應明確告知當事人事項；第 10 條：應依當事人請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本；第 11 條：應維護個人資料之正確，並應主動或依當事人請求更正或補充；第 13 條：機關受理當事人請求，應准駁之決定；第 14 條：查詢或請求閱覽個人資料或製給複製本者，得酌收必要成本費用。
2	個人資料蒐集、處理或利用等作業委外時，對於受委託者之管理	1.檢視所有個人資料處理作業委外合約或其他正式文件內容,需至少包括下列要求： - 受委託者應建立隱私權政策，並遵循委託機構的隱私權政策要求 - 受委託者應簽署之保密承諾 - 受委託者應對個人資料處理作業人員進行相關教育訓練 (例如應在 XX 月 XX 日前，至少受過 X 小時的個資管理與安全維護訓練課程) - 受委託者應符合之個資管理程序與安全維護要求 (個資管理程序詳細內容與安全維護要求之等級，視該受委託者所處理之個資風險高低，可用合約附件方式說明) - 受委託者欲將個人資料處理作業再進行轉包，應事先取得原委託機構之正式許可 - 受委託者欲將個人資料處理作業再進行轉包，轉包承接方亦應符合受委託者應符合之合約條款、個資管理程序及安全維護要求 (參照至合約相關條款或附件內容) - 當契約終止時，相關之個人資料應被銷毀、交還委託機構或其指定之	第 4 條：對受機關委託蒐集、處理或利用個人資料者之管理

項次	個資管理程序需求	建議行動方案	個資法相關要求
		單位 (例如合約終止前受委託者應將保有的個人資料全數交還委託機關，並在合約終止後 x 日內完成銷毀作業並提供銷毀過程紀錄予委託機關) - 規範履約過程中及合約終止後，委託機構可適時監督與稽核受委託者之相關作業 (包括進行考核測試、現場稽核、教育訓練，或其他可行之監督方式等) - 倘因受委託者違反個人資料保護法而遭任何其他第三人向委託機構主張任何權利、請求、索賠或訴訟等，除因委託機構之故意或重大過失行為所致者外，受委託者同意補償並確保委託機構(包括委託機構人員)不遭受亦不負擔任何索賠、責任、費用及損失	
3	檢視目前所保有之個人資料檔案是否符合正當合理蒐集目的之最少欄位需求	1.檢討現行個人資料檔案中的必填欄位／選填欄位之定義是否妥當 2.修正上述檢視後所識別出之應調整內容的相關表單與作業程序文件	第 5 條：個人資料之蒐集、處理或利用不得逾越特定目的之必要範圍 第 6 條：不得蒐集、處理或利用之個人資料
4	建立個資蒐集告知作業程序與範本	1.規劃個資蒐集流程告知作業程序 2.檢討現行個人資料檔案中的保存期限是否妥當 3.設計告知事項內容通用範本，至少包括： 一、蒐集機構名稱(A 機關) 二、蒐集之目的(依個人資料檔案列表中[特定目的]進行說明) 三、個人資料之類別(依個人資料檔案列表中[類別]進行說明) 四、個人資料利用之期間、地區、對象及方式(依個人資料檔案生命週期中[保存期限]、[個人資料檔案生命週期活動]進行說明) 五、當事人依個資法第三條規定得行使之權利及方式(同建議行動方案之[項次 1]內容) 六、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	第 8 條：向當事人蒐集個人資料時，應明確告知當事人之事項

項次	個資管理程序需求	建議行動方案	個資法相關要求
5	確認經由間接蒐集的個人資料檔案之告知程序是否完整	1.檢視個人資料檔案生命週期中[蒐集方式]為間接之個人資料檔案，是否於先前蒐集時向當事人告知相關利用之範圍已涵蓋此後續間接蒐集作業或符合下列得免告知之情況之一： - 已取得當事人書面同意 - 依法律規定得免告知 - 個人資料之蒐集係公務機關執行法定職務所必要 - 告知將妨害公務機關執行法定職務 - 告知將妨害第三人之重大利益 - 當事人明知應告知之內容 - 當事人自行公開或其他已合法公開之個人資料 - 不能向當事人或其法定代理人為告知 - 基於公共利益為統計或學術研究之目的而有必要，且該資料須處理，無從識別特定當事人者 - 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料 2.若先前並無告知或告知情況未包括上述項目,則應規劃間接蒐集之告知方式(整合建議行動方案[項次 4]之程序)	第 9 條：非直接蒐集之個人資料，於處理或利用前應向當事人告知之事項

項次	個資管理程序需求	建議行動方案	個資法相關要求
6	確立個人資料檔案之機密等級與對應之資訊安全處理原則	1.檢視機關內現有之文件(資訊)機密等級相關資訊安全處理原則與程序內容，對含有個人資料之檔案建議應列為密級以上之機密等級 2.對個人資料檔案之資訊安全處理原則與程序，應至少涵蓋下列內容： - 個人資料檔案於人員個人電腦或工作桌面之暫存或儲存或複製 - 個人資料檔案於人員個人電腦或工作桌面之刪除或銷毀 - 個人資料檔案進行內外部傳送時之資料加密或書面彌封 - 可攜式儲存裝置(包括 USB 隨身碟、行動硬碟、手持媒體及通信設備等)之使用限制與管理 - 機關保有個人資料檔案之儲存與備份 - 機關保有個人資料檔案之刪除與銷毀 - 機關保有個人資料檔案之內外部傳送 - 機關保有個人資料檔案之處理紀錄管理 3.確立機關內負責個人資料檔案安全維護之角色職責	第 11 條：應維護個人資料之正確...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； 第 18 條：公務機關應指定專人辦理安全維護事項； 第 28 條：公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限

項次	個資管理程序需求	建議行動方案	個資法相關要求
7	建立個資事故通報與處理作業程序和範本	1.規劃個資事故通報與處理作業程序(若機關已有資安事故通報與處理程序，建議整合) 2.設計個資事故紀錄單範本，建議包括： - 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 - 影響範圍(包括系統、人員、組織) - 可能影響之當事人範圍與人數 - 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 - 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)	第 12 條：個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人； 第 28 條：公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限
8	進行公務機關應於電腦網站公開，或以其他適當方式供公眾查閱之公開事項	1.確認公開之網站位置或方式 2.確認網站內容新增或更新作業程序 3.確認預定公開日期 4.提供公開資訊予網站維護人員進行公布，資訊內容應包括： - 個人資料檔案名稱 - 保有機關名稱及聯絡方式 - 個人資料檔案保有之依據及特定目的 - 個人資料之類別	第 17 條：公務機關應公開於電腦網站，或以其他適當方式供公眾查閱之事項(其有變更者，亦同)

資料來源： 本計畫整理

5. 結論

個資法於 99 年 4 月 27 日三讀通過，在保障個人隱私資料並兼顧新聞自由平衡下邁向新的里程碑。個資法強化個資揭露、查詢及更正等自主控制，同時也參考「亞太經濟合作論壇(APEC)隱私保護綱領」所揭示的預防損害、告知及蒐集限制等原則並納入規範，以迎接個資保護全球化時代的來臨。

個資法的通過，除使我國與國際接軌的程度更加緊密結合外，同時也保障個人資料不被濫用，包括一般民眾於辦完信用卡後，接到詢問是否有資金需求或保險需求的電話？家中有新生兒誕生的父母，接到詢問是否有新生兒用品、奶粉或保險的需求？剛畢業的中學生，在畢業後接獲補習班的電話，詢問是否有補習的需求？讓我們感受到個人資料未被妥善的保護與使用。

所以，個資法對於民眾的個人資料保護，將有一定的成效。對於政府機關而言，則應審慎評估與個資法相關規定，包括訂定機關之個人資料保護管理要點、指定「專人」辦理個人資料安全維護事項、設置「個資保護聯絡窗口」及指定「召集人」等。同時考量與機關已建立之資訊安全管理制度互相結合，以利統一執行管理審查相關作業，在對機關衝擊最小的情況下，順利完成個資法的防護要求。

因此，本指引發展之主要目的為以資通安全角度，協助政府機關執行個人資料保護相關作業，藉由個資保護管理建置流程，包括規劃、執行、檢查及行動四個階段，循序漸進完成個資保護管理制度。規劃階段，主要針對組織內個資管理現況、內外環境的個資需求及組織作業流程中可能與個資相關的項目，進行整體瞭解，並架構出個資管理所需之功能性組織，另藉由整合本階段所產出之個資管理現況評估結果，進行個資隱私衝擊與風險評估，藉此瞭解組織所蒐集、處理及利用的相關個資之風險係數，並對應至適當的安全控制項目基準值，做為發展風險處理對策與技術控制措施，

以及後續個資管理與防護實作的依據。執行階段，係承接規劃階段，主要活動為確立人員權責角色、建立個資管理程序、建立安全控制措施、個資委外作業管理及規劃宣導與教育訓練。檢查階段之活動，包括個資管理報告檢視、個資管理稽核活動及個資事故追蹤處理。行動階段之活動，包括管理組織審查會議及個資管理改善計畫。

政府機關於完成個資保護管理建置流程後，宜使用附件 1「個資保護管理建流程檢核表」檢視各項程序的執行情形，同時於建置初期可加強個資稽核作業，確保個資管理措施已落實於日常業務中。最後，可考量提供適當的資源，頒布個資獎勵規範，以達事半功倍之成效。此外，為便利機關快速瞭解本指引之個人資料保護架構，提供「個人資料保護參考指引導引手冊」詳如附件 16。

6. 參考文獻

[1] 行政院國家資通安全會報技術服務中心，個資保護規劃與實作建議報告，100 年。

[2] 中華民國個人資料保護法，99 年。

[3] 行政院國家資通安全會報，資訊系統分類分級與鑑別機制，99 年。http://www.nicst.nat.gov.tw/content/application/nicst/general/guest-cnt-browse.php?cnt_id=1892

[4] 行政院國家資通安全會報技術服務中心，資訊系統風險評鑑參考指引，99 年。

[5] 行政院國家資通安全會報，公務機密資料防護研究期末報告，98 年

[6] Organization for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980-09-23.

[7] Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework, 2005

[8] BSi, BS 10012:2009, Data protection – Specification for a personal information management system, May 2009

[9] ISO 22307 Financial services – Privacy impact assessment, 2008-05-01

[10] Information Commissioner's Office (ico.), Privacy Impact Assessment handbook version 2, June 2009

[11] National Institute of Standards and Technology (NIST), Special Publication 800-122, Guide to Protecting the Confidentiality of Personal Identifiable Information (PII), April 2010

[12] National Institute of Standards and Technology (NIST), Special Publication 800-53, Recommended Security Controls for Federal Information Systems (Revision 2), December 2007

[13] http://www.tecsols.com/index.php/promotional-activities/webcasts/326-protec

tion-of-personal-datanov

7. 附件

7.1. 附件 1 個資保護管理建置流程檢核表

7.2. 附件 2 個人資料保護管理要點範例

7.3. 附件 3 個人資料保護與隱私政策範例

7.4. 附件 4 個資管理整體準備度評估問卷

7.5. 附件 5 個資項目個資衝擊分析檢核表

7.6. 附件 6 個資項目衝擊分析表

7.7. 附件 7 資安事故通報與紀錄表範例

7.8. 附件 8 稽核計畫範例

7.9. 附件 9 稽核查核表範例

7.10. 附件 10 稽核紀錄範例

7.11.附件 11 個資項目技術安全控制措施基準值評估表

7.12.附件 12 委外作業稽核計畫範例

7.13.附件 13 委外作業稽核紀錄範例

7.14.附件 14 個資認知宣導海報範例

7.15.附件 15 預防與矯正行動方案範例

7.16.附件 16 個人資料保護參考指引導引手冊