貴單位個人資料盤點及風險評估作業計畫

貴　單　位　資　訊　中　心

中　華　民　國　102　年　07　月　01　日

目　錄

壹、計畫目的

為因應「個人資料保護法」、「個人資料保護法施行細則」以及　貴單位個人資料保護管理要點等法規之要求，爰建立　貴單位個人資料檔盤點與風險評估管理規範，提供　貴單位共同遵行之風險評估標準，採取適當之解決對策或控制措施，以有效降低個人資料檔案遭受損害的風險。

一、個人資料盤點目的

能有效清查及鑑別個人資料之名稱、類別(個資欄位)、保有依據、保有單位、特定目的、存在形態(書面/電子)、個資使用行為及相關利害關係人等。

二、個人資料風險評估目的

鑑別個人資料所存在之各項衝擊及威脅所導致之風險，並依據風險評估之結果採取技術面及管理面之對策(接受、降低、轉移、迴避風險)或安全控制措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

貳、計畫適用範圍

本計畫適用範圍為　貴單位○○個單位(如下表所示)之各項業務相關作業流程所產生之個人資料檔案。

表 1　貴單位各單位一覽表

No	單位名稱	No	單位名稱	No	單位名稱
1	○○○	10	○○○	19	○○○
2	○○○	11	○○○	20	○○○
3	○○○	12	○○○	21	○○○
4	○○○	13	○○○	22	○○○
5	○○○	14	○○○	23	○○○
6	○○○	15	○○○	24	○○○
7	○○○	16	○○○	25	○○○
8	○○○	17	○○○	26	○○○
9	○○○	18	○○○	27	○○○

參、時程規劃

以下列出　貴單位各單位個人資料盤點及風險評估作業之時程規劃，工作總時程約須歷時九個月，各項工作項目之時程與內容如下所述：

表 2　個資盤點與風險評估作業時程規劃

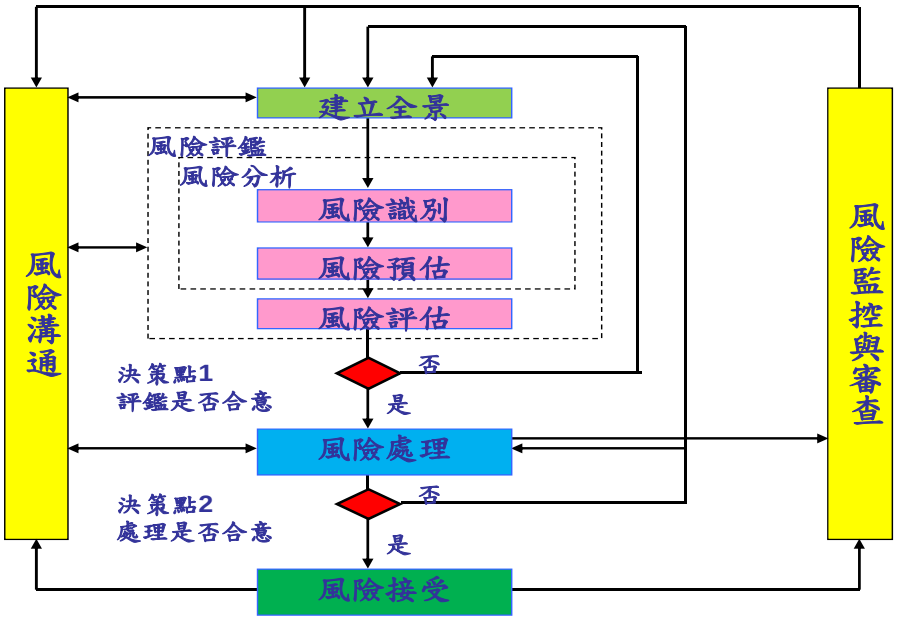
項次	工作項目	工作執行日	工作時程
1	作業文件內容確認	專案啟動後立即執行	30 個日曆天
2	辦理教育訓練	專案啟動後一個月執行	60 個日曆天
3	各單位實地輔導	專案啟動後三個月執行	150 個日曆天
4	各單位產製盤點表及評估報告	專案啟動後四個月執行	135 個日曆天
5	執行稽核查檢作業	專案啟動後八個月執行	30 個日曆天

肆、計畫內容

以下列出本計畫個人資料盤點及風險評估之方法論與執行作業流程，讓　貴單位於執行本計畫時有一明確之依據，確保計畫執行之進度與品質。

一、個資盤點及風險評估方法論

本專案依據ISO/IEC 27005：2011資訊安全風險管理之機制，建立資訊資產風險評估架構。詳見下圖所示。

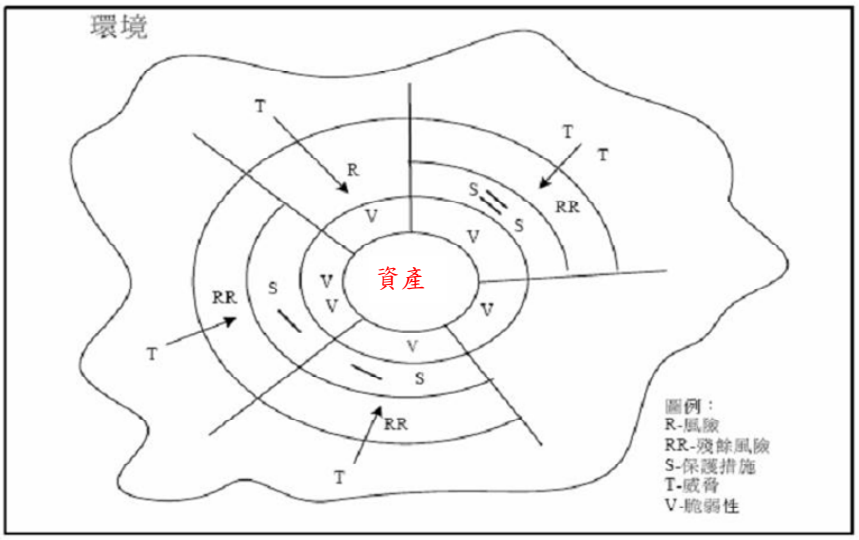


資料來源：ISO/IEC 27005：2011

圖 1　ISO/IEC 27005：2011 資訊安全風險管理架構

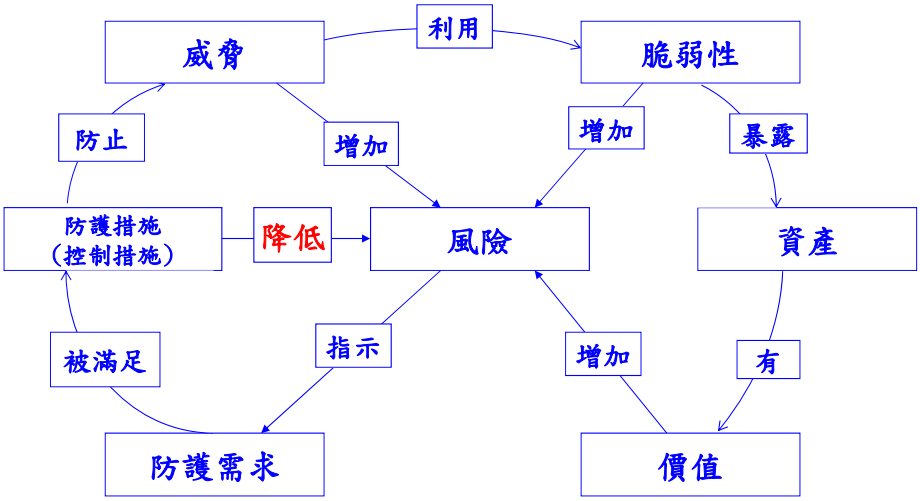
依據ISO/IEC27005之要求，需要識別資產、威脅、現有控制措施、脆弱性，並識別可能造成之後果。風險評估之概念源自於ISO/IEC13335-1，其係以資產為核心，而資產內部存在有若干之脆弱性(V)，外部有許多之威脅(T)。評估已知威脅利用脆弱性之可能性，及對資產造成衝擊之程度，稱之為風險評估。

要降低風險，需要藉助控制措施(S)的施行，才可以拒止威脅或是消除脆弱性。風險可能無法完全去除，剩餘之風險稱之為殘餘風險(RR)，採行控制措施之重點在於要將殘餘風險降低至可接受之水準。



資料來源：CNS 14929-1

圖 2　風險安全元件關係圖



資料來源：CNS 14929-1

圖 3　風險管理要素關聯圖

二、個資盤點及風險評估作業流程

建立「個資檔案風險評估與管理作業程序」，作業流程、權責單位及相關表件，如下所述：

作業流程	權責單位	相關文件
個人資料盤點(鑑別)	各單位/輔導廠商	個資項目盤點表
個資風險評估分析	各單位/輔導廠商	個資檔案風險評估彙整表
個資風險等級判定	各單位/輔導廠商	個資檔案風險處理計畫
撰寫風險評估報告	各單位/輔導廠商	個資風險評估報告
執行稽核檢查	個資保護稽核小組	
紀錄保存	各單位	

圖 4　個資檔案風險評估與管理流程圖

(一)、個人資料盤點(鑑別)

個人資料之範圍，應考量機關個資來源、個人資料類別、內部處理所涉及的角色、流程、期間、地區、利用對象與方式，最終應確認特定目的之範圍，內容詳見下圖所示。

圖 5　界定個人資料之範圍

1、貴單位各單位個資保護專責人員應協調單位同仁進行轄管業務個人資料盤點作業，並視實際狀況進行內容調整。

2、依據業務流程分析結果，執行個人資料檔案鑑別作業，並建立「個資項目盤點表」(詳如附件一)。

3、除每年執行一次個人資料檔案鑑別作業外，應於　貴單位組織變更或作業流程改變時，針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別作業。

4、「個資項目盤點表」中之「特定目的」與「個人資料類別」2欄位，應依據法務部「個人資料保護法之特定目的及個人資料之類別」之內容詳實填寫(詳如附件二)。

5、依據「個人資料保護法」第十七條規定，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。　貴單位各單位所產製之「個資項目盤點表」其內容除第十七條應公開事項外，尚列出在個資保護生命週期中之蒐集、處理、利用、保存、銷毀及揭露等各項須監控與管理之訊息，以符

合個資法及其施行細則之要求，「個資項目盤點表」僅提供　貴單位各單位內部使用。

No.	個資法第17條應公開事項
1	個人資料檔案名稱
2	保有機關名稱及聯絡方式
3	個人資料檔案保有之依據及特定目的
4	個人資料之類別

(二)、個資風險評估分析

1、風險評估執行時機

個人資料檔案風險評估作業應於每年內部稽核活動前執行。除每年執行一次外，亦應於發生：營運組織變更、作業流程改變、新增或變更個人資料檔案、發生重大個資外洩事件時，針對變動範圍內的作業程序與個人資料檔案進行風險評估。

2、風險評估分析

建立風險評量的標準(如下表所示)，包括：風險發生之機率與影響/衝擊之程度。個人資料檔案之風險評估應依據實際狀況，對照「影響及衝擊等級表」及「風險發生可能性等級表」之內容，並於「個資檔案風險評估彙整表」中進行六個評估構面之風險分析。

表 3　影響及衝擊等級表

評估項目(構面)	影響及衝擊等級表(I)		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個資查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	可以間接識別特定當事人者	可以直接識別特定當事人者
個資數量	20 筆以下 (團體訴訟不成立)	一般個資 21~10,000 筆 特種個資 21~1,000 筆	一般個資 10,001 筆以上 特種個資 1,001 筆以上
敏感程度	僅有識別資料，未含其他個人活動資料。	含有個人活動資料	含有特種個人資料
特定目的範圍內利用	特定目的範圍內利用	特定目的外利用之例外	特定目的外之利用
外部利用	無外部利用情形	無償委任關係外部利用	有償委任關係外部利用
國際傳輸	無國際傳輸情形	主管機關未規定之國際傳輸	主管機關訂定規定之國際傳輸
註記：評估項目參考NIST SP800-122選定，等級判定依據個資法之相關要求訂定，依據以上項目分項判定，最後依據最高衝擊原則，判定衝擊程度等級。			

表 4　風險發生可能性等級表

等級	可能性	發生機率	描述
3(高)	幾乎確定	61-100%	在大部分的情況下會發生
2(中)	可能	41-60%	有些情況下會發生
1(低)	幾乎不可能	0-40%	只會在特殊的情況下發生

各單位須針對各項個人資料之使用及控管狀況，依據「影響及衝擊等級表」之各個構面，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「個資檔案風險評估彙整表」(詳如附件三)。

3、風險值計算

識別風險發生之可能性(P)及影響/衝擊程度(I)，將此 2 項評分進行相乘，即求出該個人資料檔案之風險值。風險值(R) = P × I。

4.風險分布矩陣

將經由風險值計算公式所得之風險值，對應至「風險分布矩陣」以判斷風險值之分布情況。

表 5　風險分布矩陣

風險分布矩陣			
	發生機率		
影響/衝擊程度	幾乎不可能(1)	可能(2)	幾乎確定(3)
非常嚴重(3)	**3(中度)**	**6(高度)**	**9(極高度)**
嚴重(2)	**2(低度)**	**4(中度)**	**6(高度)**
輕微(1)	**1(低度)**	**2(低度)**	**3(中度)**

(三)、個資風險等級判定

1、決定可接受風險值

以下列出可接受及不可接受之風險等級，作為　貴單位各單位後續風險處理之依據。

表 6　風險判別與處理

風險值(R)	風險等級	風險判別與處理	
1 或 2	**1**	**可接受風險**	**接受**
3 或 4	**2**	**可接受風險**	**持續監視**
6 或 9	**3**	**不可接受風險**	**立即控制**

各單位個人資料風險評估可接受之風險等級，每年需檢討並經「個人資料保護管理執行小組」開會決議並記載於會議紀錄中。

2、個人資料風險處理作業

(1).依個人資料風險評估結果及可接受風險值之決議，由各風險項目負責人針對需降低風險值之個人資料擬訂「個資風險處理計畫」(詳如附件四)，以期將風險降至可接受等級。

(2).個人資料風險處理計畫之風險處理措施，應根據「個人資料保護法」對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源。

(3).個人資料風險處理計畫應提報「個人資料保護管理執行小組」審查後執行，並列入追蹤管理。

3、風險處理計畫執行成效暨殘餘風險處理

風險處理計畫於預訂完成日期結束後，須由各單位執行風險再評估，以確認風險處理計畫之執行是否達到預期目標。

(四)、撰寫風險評估報告

各單位依據個人資料檔案風險評估結果，撰寫「個資風險評估報告」(詳如附件五)，並陳單位主管確認。

三、辦理教育訓練

專案啟動後一個月，開始針對　貴單位辦理五個梯次之個資盤點及風險評估作業之訓練課程。

表 7　教育訓練課程計畫表

課程名稱	時數	梯次	時數小計	上課對象
個人資料盤點與風險評估訓練課程	2	5	10	貴單位全體同仁

四、實地輔導

專案啟動後三個月，由輔導顧問向　貴單位各單位確認輔導時間，進行實地輔導工作，協助各單位進行個資檔案盤點及風險評估作業，並產製及確認「個資項目盤點表」及「個資風險評估報告」。

五、執行稽核檢查

為查驗　貴單位各單位是否依據本計畫落實執行個資盤點及風險評估各項作業，以符合本計畫之目的，確保　貴單位保有的個人資料檔案均能落實執行相關個資保護措施，依據　貴單位「資訊安全稽核管理作業規範」及「個資保護內部稽核作業程序」之作業流程進行稽核工作。

1、擬定稽核計畫

權責人員於執行稽核前，應擬妥「個資內部稽核計畫」(詳如附件六)，並經權責主管核准後實施。計畫內容須包含：受稽核單位、稽核時程、稽核範圍、稽核人員安排...等。

2、稽核標的

稽核重點主要是查驗各單位是否如期如質產出「個資項目盤點表」及「個資風險評估報告」。

伍、附件

附件一、個資項目盤點表

附件二、個人資料保護法之特定目的及個人資料之類別

附件三、個資檔案風險評估彙整表

附件四、個資風險處理計畫

附件五、各單位個資風險評估報告

附件六、個資內部稽核計畫

相關附件

附件一

個資項目盤點表

單位名稱：　　填表日期：　　年　　月　　日

編號	個人資料檔案名稱	保有依據	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	蒐集			處理			利用			保存		銷毀		揭露		
								來源	方式	單位	方式	單位	期間	地區	單位	方式	單位	期限	形式	頻率	對象	方式	個資範圍

填表人:　　單位主管:

個人資料保護法之特定目的及個人資料之類別

代號	修正特定目的項目
○○一	人身保險
○○二	人事管理(包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施)
○○三	入出國及移民
○○四	土地行政
○○五	工程技術服務業之管理
○○六	工業行政
○○七	不動產服務
○○八	中小企業及其他產業之輔導
○○九	中央銀行監理業務
○一○	公立與私立慈善機構管理
○一一	公共造產業務
○一二	公共衛生或傳染病防治
○一三	公共關係
○一四	公職人員財產申報、利益衝突迴避及政治獻金業務
○一五	戶政
○一六	文化行政
○一七	文化資產管理
○一八	水利、農田水利行政
○一九	火災預防與控制、消防行政
○二○	代理與仲介業務
○二一	外交及領事事務
○二二	外匯業務
○二三	民政
○二四	民意調查
○二五	犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務
○二六	生態保育
○二七	立法或立法諮詢
○二八	交通及公共建設行政
○二九	公民營(辦)交通運輸、公共運輸及公共建設
○三○	仲裁
○三一	全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險
○三二	刑案資料管理

〇三三　多層次傳銷經營
〇三四　多層次傳銷監管
〇三五　存款保險
〇三六　存款與匯款
〇三七　有價證券與有價證券持有人登記
〇三八　行政執行
〇三九　行政裁罰、行政調查
〇四〇　行銷(包含金控共同行銷業務)
〇四一　住宅行政
〇四二　兵役、替代役行政
〇四三　志工管理
〇四四　投資管理
〇四五　災害防救行政
〇四六　供水與排水服務
〇四七　兩岸暨港澳事務
〇四八　券幣行政
〇四九　宗教、非營利組織業務
〇五〇　放射性物料管理
〇五一　林業、農業、動植物防疫檢疫、農村再生及土石流防災管理
〇五二　法人或團體對股東、會員(含股東、會員指派之代表)、董事、監察人、理事、監事或其他成員名冊之內部管理
〇五三　法制行政
〇五四　法律服務
〇五五　法院執行業務
〇五六　法院審判業務
〇五七　社會行政
〇五八　社會服務或社會工作
〇五九　金融服務業依法令規定及金融監理需要，所為之蒐集處理及利用
〇六〇　金融爭議處理
〇六一　金融監督、管理與檢查
〇六二　青年發展行政
〇六三　非公務機關依法定義務所進行個人資料之蒐集處理及利用
〇六四　保健醫療服務
〇六五　保險經紀、代理、公證業務
〇六六　保險監理
〇六七　信用卡、現金卡、轉帳卡或電子票證業務
〇六八　信託業務
〇六九　契約、類似契約或其他法律關係事務

○七○	客家行政
○七一	建築管理、都市更新、國民住宅事務
○七二	政令宣導
○七三	政府資訊公開、檔案管理及應用
○七四	政府福利金或救濟金給付行政
○七五	科技行政
○七六	科學工業園區、農業科技園區、文化創業園區、生物科技園區或其他園區管理行政
○七七	訂位、住宿登記與購票業務
○七八	計畫、管制考核與其他研考管理
○七九	飛航事故調查
○八○	食品、藥政管理
○八一	個人資料之合法交易業務
○八二	借款戶與存款戶存借作業綜合管理
○八三	原住民行政
○八四	捐供血服務
○八五	旅外國人急難救助
○八六	核子事故應變
○八七	核能安全管理
○八八	核貸與授信業務
○八九	海洋行政
○九○	消費者、客戶管理與服務
○九一	消費者保護
○九二	畜牧行政
○九三	財產保險
○九四	財產管理
○九五	財稅行政
○九六	退除役官兵輔導管理及其眷屬服務照顧
○九七	退撫基金或退休金管理
○九八	商業與技術資訊
○九九	國內外交流業務
一○○	國家安全行政、安全查核、反情報調查
一○一	國家經濟發展業務
一○二	國家賠償行政
一○三	專門職業及技術人員之管理、懲戒與救濟
一○四	帳務管理及債權交易業務
一○五	彩券業務
一○六	授信業務

一〇七　採購與供應管理
一〇八　救護車服務
一〇九　教育或訓練行政
一一〇　產學合作
一一一　票券業務
一一二　票據交換業務
一一三　陳情、請願、檢舉案件處理
一一四　勞工行政
一一五　博物館、美術館、紀念館或其他公、私營造物業務
一一六　場所進出安全管理
一一七　就業安置、規劃與管理
一一八　智慧財產權、光碟管理及其他相關行政
一一九　發照與登記
一二〇　稅務行政
一二一　華僑資料管理
一二二　訴願及行政救濟
一二三　貿易推廣及管理
一二四　鄉鎮市調解
一二五　傳播行政與管理
一二六　債權整貼現及收買業務
一二七　募款（包含公益勸募）
一二八　廉政行政
一二九　會計與相關服務
一三〇　會議管理
一三一　經營郵政業務郵政儲匯保險業務
一三二　經營傳播業務
一三三　經營電信業務與電信加值網路業務
一三四　試務、銓敘、保訓行政
一三五　資(通)訊服務
一三六　資(通)訊與資料庫管理
一三七　資通安全與管理
一三八　農產品交易
一三九　農產品推廣資訊
一四〇　農糧行政
一四一　遊說業務行政
一四二　運動、競技活動
一四三　運動休閒業務
一四四　電信及傳播監理

一四五	僱用與服務管理
一四六	圖書館、出版品管理
一四七	漁業行政
一四八	網路購物及其他電子商務服務
一四九	蒙藏行政
一五〇	輔助性與後勤支援管理
一五一	審計、監察調查及其他監察業務
一五二	廣告或商業行為管理
一五三	影視、音樂與媒體管理
一五四	徵信
一五五	標準、檢驗、度量衡行政
一五六	衛生行政
一五七	調查、統計與研究分析
一五八	學生（員）(含畢、結業生)資料管理
一五九	學術研究
一六〇	憑證業務管理
一六一	輻射防護
一六二	選民服務管理
一六三	選舉、罷免及公民投票行政
一六四	營建業之行政管理
一六五	環境保護
一六六	證券、期貨、證券投資信託及顧問相關業務
一六七	警政
一六八	護照、簽證及文件證明處理
一六九	體育行政
一七〇	觀光行政、觀光旅館業、旅館業、旅行業、觀光遊樂業及民宿經營管理業務
一七一	其他中央政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七二	其他公共部門(包括行政法人、政府捐助財團法人及其他公法人)執行相關業務
一七三	其他公務機關對目的事業之監督管理
一七四	其他司法行政
一七五	其他地方政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七六	其他自然人基於正當性目的所進行個人資料之蒐集處理及利用
一七七	其他金融管理業務
一七八	其他財政收入

一七九　其他財政服務
一八〇　其他經營公共事業(例如:自來水、瓦斯等)業務
一八一　其他經營合於營業登記項目或組織章程所定之業務
一八二　其他諮詢與顧問服務

代　號　識別類：

C〇〇一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C〇〇二　辨識財務者。

例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

C〇〇三　政府資料中之辨識者。

例如：身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

代　號　特徵類：

C〇一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍、聲音等。

C〇一二　身體描述。

例如：身高、體重、血型等。

C〇一三　習慣。

例如：抽煙、喝酒等。

C〇一四　個性。

例如：個性等之評述意見。

代　號　家庭情形：

C〇二一　家庭情形。

例如：結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。

C〇二二　婚姻之歷史。

例如：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。

C〇二三　家庭其他成員之細節。

例如：子女、受扶養人、家庭其他成員或親屬、父母、同居人及旅居國外及大陸人民親屬等。

C〇二四　其他社會關係。

例如：朋友、同事及其他除家庭以外之關係等。

代　　號　社會情況：

C〇三一　住家及設施。

例如：住所地址、設備之種類、所有或承租、住用之期間、租金或稅率及其他花費在房屋上之支出、房屋之種類、價值及所有人之姓名等。

C〇三二　財產。

例如：所有或具有其他權利之動產或不動產等。

C〇三三　移民情形。

例如：護照、工作許可文件、居留證明文件、住居或旅行限制、入境之條件及其他相關細節等。

C〇三四　旅行及其他遷徙細節。

例如：過去之遷徙、旅行細節、外國護照、居留證明文件及工作證照及工作證等相關細節等。

C〇三五　休閒活動及興趣。

例如：嗜好、運動及其他興趣等。

C〇三六　生活格調。

例如：使用消費品之種類及服務之細節、個人或家庭之消費模式等。

C〇三七　慈善機構或其他團體之會員資格。

例如：俱樂部或其他志願團體或持有參與者紀錄之單位等。

C〇三八　職業。

例如：學校校長、民意代表或其他各種職業等。

C〇三九　執照或其他許可。

例如：駕駛執照、行車執照、自衛槍枝使用執照、釣魚執照等。

C〇四〇　意外或其他事故及有關情形。

例如：意外事件之主體、損害或傷害之性質、當事人及證人等。

C〇四一　法院、檢察署或其他審判機關或其他程序。

例如：關於資料主體之訴訟及民事或刑事等相關資料等。

代　　號　教育、考選、技術或其他專業：

C〇五一　學校紀錄。

例如：大學、專科或其他學校等。

C〇五二　資格或技術。

例如：學歷資格、專業技術、特別執照（如飛機駕駛執照等）、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。

C〇五三　職業團體會員資格。

例如：會員資格類別、會員資格紀錄、參加之紀錄等。

C〇五四　職業專長。

例如：專家、學者、顧問等。

C〇五五　委員會之會員資格。

例如：委員會之詳細情形、工作小組及會員資格因專業技術而產生之情形等。

C〇五六　著作。

例如：書籍、文章、報告、視聽出版品及其他著作等。

C〇五七　學生(員)、應考人紀錄。

例如：學習過程、相關資格、考試訓練考核及成績、評分評語或其他學習或考試紀錄等。

C〇五八　委員工作紀錄。

例如：委員參加命題、閱卷、審查、口試及其他試務工作情形記錄。

代　　號　受僱情形：

C〇六一　現行之受僱情形。

例如：僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。

C〇六二　僱用經過。

例如：日期、受僱方式、介紹、僱用期間等。

C〇六三　離職經過。

例如：離職之日期、離職之原因、離職之通知及條件等。

C〇六四　工作經驗。

例如：以前之僱主、以前之工作、失業之期間及軍中服役情形等。

C〇六五　工作、差勤紀錄。

例如：上、下班時間及事假、病假、休假、娩假各項請假紀錄在職紀錄或未上班之理由、考績紀錄、獎懲紀錄、褫奪公權資料等。

C〇六六　健康與安全紀錄。

例如：職業疾病、安全、意外紀錄、急救資格、旅外急難救助資訊等。

C〇六七　工會及員工之會員資格。

例如：會員資格之詳情、在工會之職務等。

C〇六八　薪資與預扣款。

例如：薪水、工資、佣金、紅利、費用、零用金、福利、借款、繳稅情形、年金之扣繳、工會之會費、工作之基本工資或工資付款之方式、加薪之日期等。

C〇六九　受僱人所持有之財產。

例如：交付予受僱人之汽車、工具、書籍或其他設備等。

C〇七〇　工作管理之細節。

例如：現行義務與責任、工作計畫、成本、用人費率、工作分配與期間、工作或特定工作所花費之時間等。

C〇七一　工作之評估細節。

例如：工作表現與潛力之評估等。

C〇七二　受訓紀錄。

例如：工作必須之訓練與已接受之訓練，已具有之資格或技術等。

C〇七三　安全細節。

例如：密碼、安全號碼與授權等級等。

代　　號　財務細節：

C○八一　收入、所得、資產與投資。

例如：總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。

C○八二　負債與支出。

例如：支出總額、租金支出、貸款支出、本票等信用工具支出等。

C○八三　信用評等。

例如：信用等級、財務狀況與等級、收入狀況與等級等。

C○八四　貸款。

例如：貸款類別、貸款契約金額、貸款餘額、初貸日、到期日、應付利息、付款紀錄、擔保之細節等。

C○八五　外匯交易紀錄。

C○八六　票據信用。

例如：支票存款、基本資料、退票資料、拒絕往來資料等。

C○八七　津貼、福利、贈款。

C○八八　保險細節。

例如：保險種類、保險範圍、保險金額、保險期間、到期日、保險費、保險給付等。

C○八九　社會保險給付、就養給付及其他退休給付。

例如：生效日期、付出與收入之金額、受益人等。

C○九一　資料主體所取得之財貨或服務。

例如：貨物或服務之有關細節、資料主體之貸款或僱用等有關細節等。

C○九二　資料主體提供之財貨或服務。

例如：貨物或服務之有關細節等。

C○九三　財務交易。

例如：收付金額、信用額度、保證人、支付方式、往來紀錄、保證金或其他擔保等。

C○九四　賠償。

例如：受請求賠償之細節、數額等。

代　　號　商業資訊：

Ｃ一〇一　資料主體之商業活動。

例如：商業種類、提供或使用之財貨或服務、商業契約等。

Ｃ一〇二　約定或契約。

例如：關於交易、商業、法律或其他契約、代理等。

Ｃ一〇三　與營業有關之執照。

例如：執照之有無、市場交易者之執照、貨車駕駛之執照等。

代　　號　健康與其他：

Ｃ一一一　健康紀錄。

例如：醫療報告、治療與診斷紀錄、檢驗結果、身心障礙種類、等級、有效期間、身心障礙手冊證號及聯絡人等。

Ｃ一一二　性生活。

Ｃ一一三　種族或血統來源。

例如：去氧核糖核酸資料等。

Ｃ一一四　交通違規之確定裁判及行政處分。

例如：裁判及行政處分之內容、其他與肇事有關之事項等。

Ｃ一一五　其他裁判及行政處分。

例如：裁判及行政處分之內容、其他相關事項等。

Ｃ一一六　犯罪嫌疑資料。

例如：作案之情節、通緝資料、與已知之犯罪者交往、化名、足資證明之證據等。

Ｃ一一七　政治意見。

例如：政治上見解、選舉政見等。

Ｃ一一八　政治團體之成員。

例如：政黨黨員或擔任之工作等。

Ｃ一一九　對利益團體之支持。

例如：係利益團體或其他組織之會員、支持者等。

Ｃ一二〇　宗教信仰。

Ｃ一二一　其他信仰。

代　　號　其他各類資訊：

Ｃ一三一　書面文件之檢索。

例如：未經自動化機器處理之書面文件之索引或代號等。

Ｃ一三二　未分類之資料。

例如：無法歸類之信件、檔案、報告或電子郵件等。

Ｃ一三三　輻射劑量資料。

例如：人員或建築之輻射劑量資料等。

Ｃ一三四　國家情報工作資料。

例如：國家情報工作法、國家情報人員安全查核辦法等有關資料。

附件三

個資檔案風險評估彙整表

單位名稱： 填表日期： 年 月 日

編號	個人資料檔案名稱	評鑑別	評估構面1	評估構面2	評估構面3	評估構面4	評估構面5	評估構面6	衝擊程度(I)	可能性(P)	風險		現有控制措施
			可識別性	個資數量	個資敏感程度	特定目的範圍內利用	外部利用	國際傳輸			風險值 (R)=P×I	風險等級	
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											

備註:衝擊程度(I):由6個評估構面中分項判定,最終選擇6個構面中衝擊等級最高的作為其衝擊程度(I).

填表人: 單位主管:

附件四

個資風險處理計畫

單位名稱：　　　　　　　　　　　　　　　　　　　　　填表日期：　　年　　月　　日

資產識別暨風險說明					風險處理措施		風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值 (R)=P×I	風險等級	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						

填表人:　　　　　　　　　　　　　　　　　　　　單位主管:

附件五

貴單位 Logo

貴單位名稱

(單位名稱)個資風險評估報告

中 華 民 國　　年　　月　　日

目錄

壹、個資風險評估結果統計表

個資風險評估結果統計表			
等級 3	等級 2	等級 1	合 計

備註：各風險等級之個資檔案數量。

貳、個資檔案風險評估彙整表

個資檔案風險評估彙整表

單位名稱：　　　　填表日期：　年　月　日

編號	個人資料檔案名稱	評鑑別	評估構面1	評估構面2	評估構面3	評估構面4	評估構面5	評估構面6	衝擊程度(I)	可能性(P)	風險		現有控制措施
			可識別性	個資數量	個資敏感程度	特定目的範圍內利用	外部利用	國際傳輸			風險值(R)=P×I	風險等級	
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											

備註:衝擊程度(I):由6個評估構面中分項判定,最終選擇6個構面中衝擊等級最高的作為其衝擊程度(I).

填表人:　　　　單位主管:

参、個資風險處理計畫

個資風險處理計畫

單位名稱： 填表日期： 年 月 日

資產識別暨風險說明					風險處理措施		風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值(R)=P×I	風險等級	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						

填表人： 單位主管：

附件六

貴單位 Logo

貴單位名稱

○○○年個資內部稽核計畫

（草案）

中 華 民 國　　年　　月　　日

目　錄

壹、目的

○○○○○○（以下簡稱　貴單位）為確保各單位落實個資盤點及風險評估作業，確保個人資料受到保護，並符合法規及　貴單位相關規範之要求，爰訂定個資內部稽核計畫（以下簡稱本計畫）。

貳、稽核對象與範圍

貴單位○○個單位(如下表所示)所產製之「個資項目盤點表」及「個資風險評估報告」。

No	單位名稱	No	單位名稱	No	單位名稱
1	○○○	10	○○○	19	○○○
2	○○○	11	○○○	20	○○○
3	○○○	12	○○○	21	○○○
4	○○○	13	○○○	22	○○○
5	○○○	14	○○○	23	○○○
6	○○○	15	○○○	24	○○○
7	○○○	16	○○○	25	○○○
8	○○○	17	○○○	26	○○○
9	○○○	18	○○○	27	○○○

參、辦理方式

一、成立稽核小組及遴選稽核人員

(一)、成立個資保護稽核小組

由本計畫委外廠商及　貴單位資訊中心成立「個資保護稽核小組」，以進行個資內部稽核作業。

(二)、遴選稽核組長與稽核人員

稽核組長由各單位主管擇一擔任之，稽核人員由稽核組長選擇具有稽核經驗的人員擔任之。

No	稽核身分	姓名/聯絡方式
1	稽核組長	
2	稽核人員	

二、稽核方式

由稽核員以實地抽檢或查核（詢）方式，確認各單位是否已依規定產製「個資項目盤點表」及「個資風險評估報告」，並經單位主管確認。

三、稽核程序

依據　貴單位「資訊安全稽核管理作業規範」及「個資保護內部稽核作業程序」之規定辦理稽核工作。

肆、計畫執行工作說明

一、稽核依據

(一)、個人資料保護法。

(二)、個人資料保護法施行細則。

(三)、貴單位各單位個人資料盤點及風險評估作業計畫。

二、稽核時間

受稽單位	日期(暫定)	備　註
資訊中心	年　月　日	
國際合作處	年　月　日	
醫療品質辦公室	年　月　日	
…….	…….	

三、稽核內容

個資內部稽核查檢單，詳如附件一。

四、矯正缺失作業

於稽核時如有發現缺失，稽核員須通知當場或限期改善，並議定缺失矯正之期限。

五、內部稽核結案檢討

稽核人員將稽核工作結果彙整，並進行稽核結果之總結報告，並提出檢討與未來改進措施。

伍、其他相關事項

附件一、個資內部稽核查檢單

貴　單　位　名　稱
個　資　內　部　稽　核　查　檢　單

紀錄編號：

受稽單位		受稽單位代表	
稽核時間	年　月　日　時　至　年　月　日　時		
文件編號		文件名稱	

項次	內　部　稽　核　要　項	稽核紀錄(稽核發現)	稽核結果	備註
1	是否依規定完成「個資項目盤點表」並經單位主管確認?			稽核結果○：表符合規定 ╳：表不符合規定 ＼表示本項不適用
2	是否依規定完成「個資風險評估報告」並經單位主管確認?			

稽核人員：

表單填寫範例

附件一

個資項目盤點表(參考範例)

單位名稱：　　填表日期：　　年　　月　　日

編號	個人資料檔案名稱	保有依據	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	蒐集			處理			利用			保存		銷毀		揭露		
								來源	方式	單位	方式	單位	期間	地區	單位	方式	單位	期限	形式	頻率	對象	方式	個資範圍
1	員工保密切結書	依據公務員服務法-第4條保密義務	137資通安全與管理	C001 C003	姓名、地址、身分證字號	□數位 ■紙本	□是 ■否	員工填寫	■直接 □間接	○○室	系統建檔	○○室	營運期間	台灣地區	○○室	保密切結證明	○○室(分機:XXX)	7年或員工離職後銷毀	紙本碎紙	每年檢視員工離職後可銷毀	無	無	無
2	醫療資訊系統	醫療法第67條	012公共衛生或傳染病防治 064保健醫療服務	C001 C003 C011 C012 C013 C021 C066 C111 C112 C113	姓名,生日,年齡,性別,身分證字號,國籍,電話,地址,身高,體重,血型,婚姻,教育程度,家族史,健康記錄,性生活,種族	■數位 □紙本	■是(病歷、醫療、健康記錄) □否	病人填寫	■直接 □間接	醫○科	系統建檔	醫○科	營運期間	台灣地區	醫○科	醫療業務使用	○○科(分機:XXX)	營運期間內	電子檔刪除	營運終止後立即銷毀	無	無	無
3	診斷書開立	醫療法	064保健醫療服務	C001 C003	姓名,ID,生日,性別,病歷號,醫療紀錄	■數位 ■紙本	■是(病歷) □否	病歷	■直接 □間接	醫○科	系統建檔	醫○科	營運期間	台灣地區	醫○科	提供病人診斷書	○○室(分機:XXX) ○○科(分機:XXX)	營運期間內保存	電子檔刪除、紙本碎紙	營運終止後立即銷毀	病患	提供紙本文件	姓名,身分字號,生日,性別,病歷號,醫療紀錄
4	研討會廣宣名單	合約	109教育或訓練行政	C001	姓名,單位,職稱,連絡電話(手機),E-amil,傳真	■數位 □紙本	□是 ■否	寄送報名表請與會人員填寫	■直接 □間接	○○組	系統建檔	○○組	營運期間	台灣地區	○○組	通訊聯繫及資料寄送	○○組(分機:XXX)	教育訓練執行期間	電子檔刪除	訓練結束後半年進行銷毀	無	無	無
5	藥師證書影本	藥師法	103專門職業及技術人員之管理	C001 C003 C039	姓名/藥師證號/生日/身分證號	■數位 ■紙本	□是 ■否	藥師	■直接 □間接	藥○科	系統建檔	藥○科	營運期間	台灣地區	藥○科	人員管理/醫院評鑑佐證	藥○科(分機:XXX)	至離職後4年	電子檔刪除、紙本碎紙	保存期限到銷燬	無	無	無

填表人:　　單位主管:

附件三

個資檔案風險評估彙整表(參考範例)

單位名稱：　　填表日期：　年　月　日

編號	個人資料檔案名稱	評鑑別	評估構面1	評估構面2	評估構面3	評估構面4	評估構面5	評估構面6	衝擊程度(I)	可能性(P)	風險		現有控制措施
			可識別性	個資數量	個資敏感程度	特定目的範圍內利用	外部利用	國際傳輸			風險值(R)=P×I	風險等級	
1	員工保密切結書	第一次評鑑	3	2	1	1	1	1	3	1	3	2	實體安全控管(鐵櫃)
		風險再評鑑											
2	醫療資訊系統資料	第一次評鑑	2	3	3	2	2	1	3	2	6	3	存取權限控管/實體(機房)與環境安全控管
		風險再評鑑											
3	診斷書開立	第一次評鑑	3	3	3	1	1	1	3	1	3	2	實體安全控管(檔案室)
		風險再評鑑											
4	研討會廣宣名單	第一次評鑑	1	2	1	1	1	1	2	2	4	2	實體安全控管(鐵櫃)
		風險再評鑑											
5	藥師證書影本	第一次評鑑	3	2	1	1	1	1	3	1	3	2	存取權限控管/實體安全控管(鐵櫃上鎖)
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											

備註:衝擊程度(I):由6個評估構面中分項判定,最終選擇6個構面中衝擊等級最高的作為其衝擊程度(I).

填表人:　　單位主管:

附件四

個資風險處理計畫(參考範例)

單位名稱：　　填表日期：　　年　　月　　日

資產識別暨風險說明					風險處理措施		風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值(R)=P×I	風險等級	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
1	醫療資訊系統資料	1. 未定期執行存取權限審查作業 2. 未落實存取權限控管機制	6	3	□接受風險 ■降低風險 □轉移風險 ■避免風險	1.每年定期執行存取權限審查作業 2.取消遠端存取作業 3.落實同仁職務異動之權限審查作業	張○○	102/06/15	102/06/09	林○○	已完成
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						

填表人:　　單位主管:

附件五

貴單位 Logo

貴單位名稱

(單位名稱)個資風險評估報告

中 華 民 國　　年　　月　　日

目錄

壹、個資風險評估結果統計表

個資風險評估結果統計表			
等級 3	等級 2	等級 1	合 計
1	4	0	5

備註：各風險等級之個資檔案數量。

貳、個資檔案風險評估彙整表

附件三

個資檔案風險評估彙整表

單位名稱： 填表日期： 年 月 日

編號	個人資料檔案名稱	評鑑別	評估構面1	評估構面2	評估構面3	評估構面4	評估構面5	評估構面6	衝擊程度(I)	可能性(P)	風險		現有控制措施
			可識別性	個資數量	個資敏感程度	特定目的範圍內利用	外部利用	國際傳輸			風險值(R)=P×I	風險等級	
1	員工保密切結書	第一次評鑑	3	2	1	1	1	1	3	1	3	2	實體安全控管(鐵櫃)
		風險再評鑑											
2	醫療資訊系統資料	第一次評鑑	2	3	3	2	2	1	3	2	6	3	存取權限控管/實體(機房)與環境安全控管
		風險再評鑑											
3	診斷書開立	第一次評鑑	3	3	3	1	1	1	3	1	3	2	實體安全控管(檔案室)
		風險再評鑑											
4	研討會廣宣名單	第一次評鑑	1	2	1	1	1	1	2	2	4	2	實體安全控管(鐵櫃)
		風險再評鑑											
5	藥師證書影本	第一次評鑑	3	2	1	1	1	1	3	1	3	2	存取權限控管/實體安全控管(鐵櫃上鎖)
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											
		第一次評鑑											
		風險再評鑑											

備註:衝擊程度(I):由6個評估構面中分項判定,最終選擇6個構面中衝擊等級最高的作為其衝擊程度(I).

填表人: 單位主管:

參、個資風險處理計畫

附件四

個資風險處理計畫

單位名稱： 填表日期： 年 月 日

資產識別暨風險說明					風險處理措施		風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值(R)=P×I	風險等級	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
1	醫療資訊系統資料	1.未定期執行存取權限審查作業 2.未落實存取權限控管機制	6	3	□接受風險 ■降低風險 □轉移風險 ■避免風險	1.每年定期執行存取權限審查作業 2.取消遠端存取作業 3.落實同仁職務異動之權限審查作業	張○○	102/06/15	102/06/09	林○○	已完成
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						
					□接受風險 □降低風險 □轉移風險 □避免風險						

填表人： 單位主管：