

經濟部標準檢驗局個人資料保護管理作業程序 部分規定修正對照表

修正規定	現行規定	說明
四、有關個人資料保護之相關用詞，依<u>個人資料保護法</u>（以下簡稱<u>本法</u>）及其施行細則規定之定義。 有關電子文件及電子簽章之相關用詞，依電子簽章法及其施行細則規定之定義。	四、有關個人資料保護之相關用詞，依<u>本法</u>及其施行細則規定之定義。 有關電子文件及電子簽章之相關用詞，依電子簽章法及其施行細則規定之定義。	修正第一項，補充有關 <u>本法</u> 為個人資料保護法之簡稱。
第九章之一 對非公務機關個人資料保護監管作業程序		一、<u>本章新增</u>。 二、為規範本局對非公務機關個人資料保護之監管作業，爰予增訂。
五十一之一、本局應依據行政院及所屬各機關落實個人資料保護聯繫作業要點（以下簡稱聯繫作業要點）規定，落實對非公務機關個人資料保護之監管，定期提報個人資料行政檢查相關計畫予本部商業發展署彙整，並依「非公務機關個人資料安全稽核檢查表」（附件二十一之一）辦理行政檢查。		一、<u>本點新增</u>。 二、定明本局對非公務機關個人資料保護監管作業之依據及執行方式，並參酌經濟部個人資料保護作業手冊內容，增訂附件二十一之一，以明確行政檢查之具體事項。
五十一之二、案件通報及處理： （一）本局於獲知所監管非公務機關發生違反個人資料檔案安全維護義務（以下簡稱個資安維案件）後，主管該非公務機關之單位（以下簡稱業管單位）應填列聯繫作業要點之「監督通報紀錄表」，並依「經濟部個人資料保護作業手冊」規定之流程辦理通報，通報時應副知本小組行政組。 （二）業管單位應就個資安維案件之後續行政措施及		一、<u>本點新增</u>。 二、為使本局業管單位於獲知所管非公務機關發生個資安維案件後，有明確之案件通報及處理機制，爰參酌經濟部個人資料保護作業手冊內容予以增訂，並以分款方式規範；第一款係有關通報時應填列之表單及辦理通報及行政調查時所遵循之流程，第二款為業管單位就後續處置

處置情形，通報本部商業發展署並副知本小組行政組；重大矚目之個資安維案件後續行政措施及處置情形，業管單位應即時通報本法主管機關及數位發展部，並副知本小組行政組。 (三) 業管單位得依本法第二十二條至第二十六條規定，對發生個資安維案件之非公務機關為適當之監督管理措施；經查明違反本法之規定者，應視行政調查結果，依本法第四十七條至第五十條規定辦理。		情形，應通報相關機關，第三款為監管措施及查明非公務機關有違反本法規定時之辦理依據，以提升案件處理效率並落實監督機制。 三、有關第二款重大矚目之範圍，依聯繫作業要點第二點第二項規定，係指行政院、立法院或監察院關注之個資安維案件或經媒體顯著披露之個資安維案件，例如經平面媒體全國性版面報導、電子媒體專題討論。
五十九、本小組行政組應於每年本局辦理資訊安全管理系統內部稽核前，向本局資通安全推動小組稽核分組提交「個人資料安全稽核檢查表」(附件二十八)，納入該年度資訊安全管理系統內部稽核作業之查核範圍。 本小組行政組得視各單位之組織編制、業務內容、年度稽核重點及其他稽核需求，根據「個人資料安全稽核檢查表」(附件二十八)之內容，進行稽核項目之增刪或調整。	五十九、本小組行政組應於每年本局辦理資訊安全管理系統內部稽核前，向本局資訊安全管理委員會稽核小組提交「個人資料安全稽核檢查表」(附件二十八)，納入該年度資訊安全管理系統內部稽核作業之查核範圍。 本小組行政組得視各單位之組織編制、業務內容、年度稽核重點及其他稽核需求，根據「個人資料安全稽核檢查表」(附件二十八)之內容，進行稽核項目之增刪或調整。	為配合本局資訊安全管理委員會及其稽核小組名稱調整，第一項酌作文字修正。

非公務機關()個人資料安全稽核檢查表

填表單位：_____

填表說明：

一、稽核結果欄：依稽核實際狀況，參考相關佐證資料填具查核結果。

(一)符合：實際作業已依稽核內容訂定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

(二)不符合：未完全依稽核內容要求訂定相關程序，或未完全依相關程序執行並產生實作紀錄；並請於說明欄儘可能詳述未符合之情形與樣態。

(三)不適用：實際作業排除稽核內容之適用。

二、說明欄位：應記錄稽核之參考佐證資料或簡述實際作業狀況。

稽核項目	稽核內容	查核結果	說明	備註
1. 配置管理之人員及相當資源	1.1 是否設個人資料管理單位或適當組織？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資管理單位組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項，如：參與會議、盤點及風險評鑑工作、事件處理等。
2. 界定個人資料之範圍	2.1 是否每年定期清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個人資料檔案清冊及個人資料作業流程說明文件，並經權責主管核定之紀錄。
3. 個人資料之風險評估及管理機制	3.1 是否每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附風險評估過程底稿、風險評鑑報告及風險處理計畫。

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

4. 事故之預防、通報及應變機制	4.1 個資事故應變機制是否包含降低、控制事故對當事人造成損害之作法？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明應變機制對降低、控制事故對當事人造成損害之作法。
	4.2 個資事故應變機制，是否包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之專線與其他查詢管道？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明應變機制對通知當事人之作法。
	4.3 個資事故應變機制，是否包含避免類似事故再次發生之矯正及預防機制？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明應變機制對避免類似事故再次發生之矯正及預防機制。
	4.4 是否就個資事件之重大事故定義，及重大事故之通報流程為何？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附事故通報文件。
5. 蒐集、處理、利用作業	5.1 資料蒐集、處理是否具備特定目的並具有法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附最新個資盤點資料，確認皆已識別保有依據。
	5.2 個人資料之利用，是否符合特定目的之範圍？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附最新個資盤點資料，確認皆已識別保有依據。
	5.3 是否有目的外之利用？目的外利用是否符合法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明機關所蒐集之個資是否具有目的外之利用情形。如有目的外利用，請說明其符合之法定要件。
	5.4 是否依規定取得當事人同意（當事人同意之	☐ 符合 ☐ 不符合 ☐ 不適用		請說明蒐集個資並取得當事人同意之情形。

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

	情形)？			
	5.5 是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附告知事項。
	5.6 是否已於首次行銷時提供當事人表示拒絕行銷之管道？如需費用是由機關支付所需費用？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明提供當事人拒絕行銷之方式。
	5.7 是否依當事人拒絕接受行銷之要求，立即停止利用其個人資料為行銷，並周知所屬人員或採行防範所屬人員再次行銷之措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明是否有當事人拒絕接受行銷以及作業流程。
6. 資料安全管理及人員管理	6.1 是否識別業務內容涉及個人資料蒐集、處理或利用之人員？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資管理單位組織圖、分工及相關辦法，以及個人資料檔案清冊。
	6.2 是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資系統權限申請表單以及帳號權限審查紀錄。
	6.3 是否與所屬人員約定保密義務？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書。
	6.4 是否要求人員離職時，返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書或離職單。

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

	6.5 消費者個人資料有加密之必要者，於蒐集、處理或利用時，是否採取適當之加密措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明針對個資電子檔案之控管規範，例如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？並檢附查核結果。
	6.6 傳輸消費者個人資料時，是否依不同傳輸方式，採取適當之安全措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明機關對外傳送個資檔案之相關規範，檢附規範制度文件。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？並請相關佐證。
	6.7 消費者個人資料有備份之必要者，是否對備份資料採取適當之保護措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明資料備份機制，並檢附規範制度文件。
7. 認知宣導及教育訓練	7.1 是否定期對實施所屬人員之個人資料保護與管理認知宣導及教育訓練？所屬人員是否明瞭上課內容？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附對所屬人員之教育訓練簡報、各項相關課程簽到表(需含授課日期)及課後評量結果。上課內容應包含個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。
8. 設備安全管理措施	8.1 是否依據作業內容及環境之不同，實施必要之安全環境管制？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明對存放儲存媒介物之環境相關消防、監控、進出入等控管措施，並檢附相關照片。
	8.2 是否妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備？	☐ 符合 ☐ 不符合 ☐ 不適用		請確認是否定期檢查或維護更新設備？並請檢附定期檢查及維護紀錄。
	8.3 是否針對不同作業環境，建置必要之保護設備或技術？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附消防、監控設備等維護紀錄。
9. 資料安全稽核機制	9.1 是否每年定期由適當組織執	☐ 符合 ☐ 不符合		請說明稽核之頻率及執行方式，並檢附最近一次之評估

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

	行資料安全內部稽核並提出評估報告？	☐ 不適用		報告。
	9.2 是否採取改善措施以持續改善資料安全維護？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附檢視或修正之紀錄，並檢附稽核矯正單及追蹤紀錄。
10. 使用紀錄、軌跡資料及證據保存	10.1 是否保存個人資料提供或移轉第三人之紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用		是否保存個人資料提供或移轉第三人之紀錄？
	10.2 是否保存當事人行使個資法第三條之權利及處理過程之紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附當事人行使個資法第三條之權利及處理過程之紀錄。
	10.3 是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。
	10.4 是否保存人員權限新增、變動及刪除之紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附人員權限新增、變動及刪除之紀錄。
	10.5 是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明留存之期限，並檢附近一年消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料。
11. 個人資料安全維護之整體持續改善	11.1 是否定期就個人資料安全維護議題召開會議並提出持續改善報告？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附相關個人資料安全維護議題會議之記錄。
	11.2 是否訂定個人資料管理	☐ 符合 ☐ 不符合		請檢附個人資料管理(或安全維護)辦法以及完整之版本資

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

	(或安全維護)辦法並定期檢視更新?	☐ 不適用		訊，包含但不限於日期、提報人及核定人等相關資訊。
12. 委託作業	12.1 委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資委外之廠商清單及合約文件。
	12.2 委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當之監督事項及方式？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資委外之廠商清單及合約文件。
	12.3 委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明對委外廠商之監督方式或檢附委外稽核報告以及稽核缺失追蹤情形。
	12.4 是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資委外之廠商清單及合約文件。
	12.5 是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附個資委外之廠商清單及合約文件。
13. 使用資通訊系統蒐集、處理或利用個人資料	13.1 是否就使用資通訊系統蒐集、處理或利用個人資料之服務範圍取得資安或	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附外部稽核證書(或驗證通過證明書)，例如 ISO 27001、27701，以確認驗證範圍包含本系統開發生命週期及對客戶提供之服務流

附件二十一之一：非公務機關個人資料安全稽核檢查表（第1版）

	個資驗證？			程，以及持續有效。
14. 個資存放雲端之安全控管	14.1 是否確保個人資料放在雲端上的安全？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明如何確認 Database 的安全以及放在那個國家？並提出相關佐證(如雲端業者出具的證明書)。
15. 發生個資事件之處理	15.1 近兩年內是否發生個人資料被竊取、洩漏、竄改或其他侵害情形之個資事件？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附通報記錄。
	15.2 是否就個資事件委請公正之第三方進行調查？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附就個資事件聘請第三方資安廠商就事件調查之報告。
	15.3 是否即時且適當的通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附向用戶說明事件緣由及防護措施之通知。
	15.4 是否就事件的發生進行根因分析，並提出強化措施？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附事件報告、強化措施的實施情形以及相關內部會議紀錄。
16. 個人資料庫之共享使用	16.1 是否有其他關係企業或主體共享使用本公司所蒐集之客戶個人資料庫？	☐ 符合 ☐ 不符合 ☐ 不適用		請說明具體共享使用之主體名稱，以及共享使用之原因及安全控管措施。另檢附告知當事人之佐證。
	16.2 是否使用其他關係企業或主體所蒐集之客戶個人資料庫加以處理及利用？	☐ 符合 ☐ 不符合 ☐ 不適用		請檢附於處理及利用前告知當事人之佐證。

修正說明：為明確行政檢查具體事項，爰增訂本附件。

第五十一點之一附件二十一之一(修正前)

無

個人資料安全稽核檢查表

填表說明：

一、稽核結果欄：依稽核實際狀況，參考相關佐證資料填具查核結果。

（一）符合：實際作業已依稽核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

（二）不符合：完全未依稽核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三）不適用：實際作業排除稽核內容之適用。

二、說明欄位：應記錄稽核之參考佐證資料，或簡述實際作業狀況。

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
1.人員及資源配置	1.1 是否已配置專責人員或組織管理及維護保有之個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	1.2 配置適當資源？	☐ 符合 ☐ 不符合 ☐ 不適用	
2.蒐集、處理、利用作業	2.1 資料蒐集、處理是否具備特定目的並具有法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.2 蒐集程序是否依規定奉簽核後為之？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.3 是否依規定取得當事人同意（當事人同意之情形）？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.4 是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.5 是否依規定簽奉核定後補充、更正個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.6 是否依規定簽奉核定後刪除、銷毀個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.7 個人資料之利用，是否符合特定目的之範圍？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	2.8 是否有目的外之利用？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.9 目的外利用是否符合法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.10 是否依規定簽奉核定後停止處理、利用個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
3.當事人權利行使程序	3.1 是否依設置當事人權利行使處理流程？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.2 受理當事人權利行使時，是否有為確認身分之動作？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.3 非當事人本人申請時，代理人是否出具相關證明文件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.4 受理申請後，是否依規定進行簽核？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.5 延長回覆期間時，是否將原因以書面通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.6 駁回當事人申請時，是否具備法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.7 駁回當事人申請時，是否以書面將拒絕事由告知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
4.盤點與風險分析	4.1 是否進行個資盤點？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.2 個資盤點是否確實？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.3 是否建立盤點清冊？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.4 是否依個資法第 17 條規定將資訊公開？	☐ 符合 ☐ 不符合 ☐ 不適用	僅稽核本局法務室及各分局。
	4.5 是否進行風險評估？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	4.6 是否製成風險評鑑表？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.7 是否針對風險進行因應？	☐ 符合 ☐ 不符合 ☐ 不適用	
5.事故通報與應變程序	5.1 是否有通報及應變程序？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.2 事故發生時是否確實通報？	☐ 符合 ☐ 不符合 ☐ 不適用	當年度無事故者，5.2-5.6 應填不適用。
	5.3 是否採取應變措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.4 是否於適當期間內通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.5 事後是否採取預防措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.6 是否作成個人資料安全事故處理報告，並簽陳本部部次長核定後，送交本部個資小組及本小組行政組備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.7 接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資安維案件，是否依聯繫作業要點規定，填列監督通報紀錄表，通報本法主管機關或數位發展部？	☐ 符合 ☐ 不符合 ☐ 不適用	僅稽核本局檢驗行政組及度量衡行政組。 有通報者，請檢附通報紀錄表。 非為負責該項業務者應填不適用。
6.認知宣導與教育訓練	6.1 是否確實進行認知宣導與教育訓練？	☐ 符合 ☐ 不符合 ☐ 不適用	
	6.2 是否進行課後評量？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	6.3 是否對新進人員進行教育訓練？	☐ 符合 ☐ 不符合 ☐ 不適用	
7.資料安全、人員管理及設備安全	7.1 是否進行去識別化作業？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.2 是否有資料存取控制措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.3 是否進行加密？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.4 資料之傳送是否進行管控？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.5 保有資料者是否遵守保密協定？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.6 人員進出情形是否具體掌控？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.7 是否對設備及環境進行控管與保護？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.8 是否定期檢查或維護更新設備？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.9 是否以適當方式（如：碎紙機銷毀、焚毀、水銷等）銷毀紙本個人資料，並視需要留存適當之銷毀紀錄？是否使用可達成適當碎紙效果（無法再拼湊或用肉眼辨識內容）之碎紙機進行個人資料之銷毀？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.10 是否以適當方式（如：低階格式化、軟體複寫、消磁或物理破壞等）銷毀存有個人資料之儲存媒體，並視需要留存適當之銷毀紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	7.11 使用、處理個人資料檔案之系統帳號，是否經申請並由權責主管核可？權限賦予是否符合業務須知（Need-to-Know）與執行工作所需合理權限原則？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.12 是否針對機關（單位）同仁及外部人員（如：合作機關（構）、廠商、工讀生等）配賦唯一的使用者識別碼並具備合適的身分鑑別措施？是否建立適當之複核機制？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.13 人員離職或職務異動時，是否由原屬權責主管審查存取授權之異動？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.14 如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.15 以電子郵件傳送敏感級以上個資檔案時，是否採加密機制，並確認加密機制之有效性？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.16 存放個人資料檔案之電腦是否定期執行各項漏洞修補程式或安全性更新？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.17 存放個人資料檔案之電腦是否全面使用防毒軟體並即時更新病毒碼？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.18 存放個人資料檔案之電腦設備委外維修或報廢時，是否	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	事先移除個人資料？		
	7.19 存放個人資料檔案之電腦設備攜出或借出時，是否經權責主管授權核准？	☐ 符合 ☐ 不符合 ☐ 不適用	
8.個人資料使用紀錄、軌跡資料及相關證據應妥善保管、定期覆核	8.1 是否對保存之個資進行紀錄（如存取及利用紀錄、調閱紀錄、軌跡資料）、證據之管理措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.2 是否定有保管期限？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.3 延長保管期限時，是否依照規定？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.4 是否依保管期限確實刪除或銷毀？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.5 因業務需求經權責主管授權執行個人資料之處理行為，是否留存包括使用者身分與其行為內容等之使用紀錄或軌跡資料以供事後查核或舉證？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.6 權責主管或管理人員，是否定期審查相關使用紀錄或軌跡資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
9.委外作業	9.1 是否有委外蒐集、處理或利用個人資料之情形並簽訂書面契約？	☐ 符合 ☐ 不符合 ☐ 不適用	當年度無委外作業者，9.1-9.5 應填不適用。
	9.2 是否將受託者之個人資料安全維護措施列入評選項目？	☐ 符合 ☐ 不符合 ☐ 不適用	
	9.3 是否定期確認受託者執行狀況，並作成紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	
	9.4 提出限期改善時，是否持續	☐ 符合 ☐ 不符合	

附件二十八：個人資料安全稽核檢查表（第4版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	追蹤改善情形？	☐ 不適用	
	9.5 契約終止或解除時，是否要求受託者確實刪除、銷毀或返還？	☐ 符合 ☐ 不符合 ☐ 不適用	
10. 資料安全稽核機制	10.1 是否訂定定期檢視各項個人資料保護措施之資料安全稽核作業機制？	☐ 符合 ☐ 不符合 ☐ 不適用	
	10.2 稽核作業結束後，是否將稽核結果製作報告備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	10.3 是否針對稽核結果進行後續改正作業，並保留矯正作業執行紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	
11. 缺失改善與矯正預防作業	11.1 是否訂定矯正及預防程序，於各類查核發現不符合、觀察或建議事項時，進行根因分析，並採取適當之矯正及預防措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	11.2 是否對各類查核發現之不符合事項之矯正與預防措施訂定合理之執行期限且追蹤執行結果，並有相關紀錄備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	11.3 針對各類查核發現之不符合事項矯正措施，是否於執行期限內完成？是否持續追蹤至改善完成？	☐ 符合 ☐ 不符合 ☐ 不適用	
12. 對非公務機關個人資料保護之監管	12.1 是否定期檢討依個資法第27條第3項訂定相關辦法之必要性？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明依聯繫作業要點第六點所列情形綜合考量之檢討結果。 已訂定相關辦法或

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
			無監管非公務機關者，應填不適用。
	12.2 已訂定相關辦法者，就該辦法所規定之事項，是否完整？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明是否依前揭作業要點訂定。 未訂定相關辦法者，應填不適用。
	12.3 是否檢視個資法第22條第1項規定之情形，採取行政檢查？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明檢視之結果。 無監管非公務機關者，應填不適用。
	12.4 採取行政檢查時，是否符合個資法第22條至第24條之規定？	☐ 符合 ☐ 不符合 ☐ 不適用	請檢附實施檢查之紀錄。 未採取行政檢查者，應填不適用。
	12.5 非公務機關有違反個資法規定之情事者，進行處分時是否符合個資法第25條之規定？	☐ 符合 ☐ 不符合 ☐ 不適用	請檢附處分書。 未採取處分者，應填不適用。
	12.6 公布非公務機關之違法情形及其姓名或名稱與負責人時，是否妥善考量相關因素？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明公布之方式並檢附公布內容。 未公布者，應填不適用。

修正說明：

- 一、因「行政院及所屬各機關落實個人資料保護聯繫作業要點」已將個資外洩案件修正為個資安維案件，並調整受通報機關，爰配合修正稽核內容5.7之文字。
- 二、考量中央流行疫情指揮中心已於112年5月1日正式解編，爰刪除稽核項目12. 配合嚴重特殊傳染性肺炎中央流行疫情指揮中心之要求，原稽核項目13修正後移列12，並配合修正12.1說明之點次。

個人資料安全稽核檢查表

填表說明：

一、稽核結果欄：依稽核實際狀況，參考相關佐證資料填具查核結果。

（一）符合：實際作業已依稽核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

（二）不符合：完全未依稽核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三）不適用：實際作業排除稽核內容之適用。

二、說明欄位：應記錄稽核之參考佐證資料，或簡述實際作業狀況。

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
1.人員及資源配置	1.1 是否已配置專責人員或組織管理及維護保有之個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	1.2 配置適當資源？	☐ 符合 ☐ 不符合 ☐ 不適用	
2.蒐集、處理、利用作業	2.1 資料蒐集、處理是否具備特定目的並具有法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.2 蒐集程序是否依規定奉簽核後為之？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.3 是否依規定取得當事人同意（當事人同意之情形）？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.4 是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.5 是否依規定簽奉核定後補充、更正個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.6 是否依規定簽奉核定後刪除、銷毀個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.7 個人資料之利用，是否符合特定目的之範圍？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第3版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	2.8 是否有目的外之利用？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.9 目的外利用是否符合法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	2.10 是否依規定簽奉核定後停止處理、利用個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
3.當事人權利行使程序	3.1 是否依設置當事人權利行使處理流程？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.2 受理當事人權利行使時，是否有為確認身分之動作？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.3 非當事人本人申請時，代理人是否出具相關證明文件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.4 受理申請後，是否依規定進行簽核？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.5 延長回覆期間時，是否將原因以書面通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.6 駁回當事人申請時，是否具備法定要件？	☐ 符合 ☐ 不符合 ☐ 不適用	
	3.7 駁回當事人申請時，是否以書面將拒絕事由告知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
4.盤點與風險分析	4.1 是否進行個資盤點？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.2 個資盤點是否確實？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.3 是否建立盤點清冊？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.4 是否依個資法第 17 條規定將資訊公開？	☐ 符合 ☐ 不符合 ☐ 不適用	僅稽核本局法務室及各分局
	4.5 是否進行風險評估？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第3版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	4.6 是否製成風險評鑑表？	☐ 符合 ☐ 不符合 ☐ 不適用	
	4.7 是否針對風險進行因應？	☐ 符合 ☐ 不符合 ☐ 不適用	
5.事故通報與應變程序	5.1 是否有通報及應變程序？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.2 事故發生時是否確實通報？	☐ 符合 ☐ 不符合 ☐ 不適用	當年度無事故者，5.2-5.6 應填不適用
	5.3 是否採取應變措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.4 是否於適當期間內通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.5 事後是否採取預防措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.6 是否作成個人資料安全事故處理報告，並簽陳本部部次長核定後，送交本部個資小組及本小組行政組備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	5.7 接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，是否於接獲通報、副知或知悉時起 72 小時內，填列監督通報紀錄表，通報國發會？	☐ 符合 ☐ 不符合 ☐ 不適用	請檢附通報紀錄表。 非為負責該項業務者應填不適用。
6.認知宣導與教育訓練	6.1 是否確實進行認知宣導與教育訓練？	☐ 符合 ☐ 不符合 ☐ 不適用	
	6.2 是否進行課後評量？	☐ 符合 ☐ 不符合 ☐ 不適用	
	6.3 是否對新進人員進行教育訓練？	☐ 符合 ☐ 不符合	

附件二十八：個人資料安全稽核檢查表（第3版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	練？	☐ 不適用	
7. 資料安全、人員管理及設備安全	7.1 是否進行去識別化作業？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.2 是否有資料存取控制措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.3 是否進行加密？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.4 資料之傳送是否進行管控？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.5 保有資料者是否遵守保密協定？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.6 人員進出情形是否具體掌控？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.7 是否對設備及環境進行控管與保護？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.8 是否定期檢查或維護更新設備？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.9 是否以適當方式（如：碎紙機銷毀、焚毀、水銷等）銷毀紙本個人資料，並視需要留存適當之銷毀紀錄？是否使用可達成適當碎紙效果（無法再拼湊或用肉眼辨識內容）之碎紙機進行個人資料之銷毀？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.10 是否以適當方式（如：低階格式化、軟體複寫、消磁或物理破壞等）銷毀存有個人資料之儲存媒體，並視需要留存適當之銷毀紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.11 使用、處理個人資料檔案	☐ 符合 ☐ 不符合	

附件二十八：個人資料安全稽核檢查表（第3版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	之系統帳號，是否經申請並由權責主管核可？權限賦予是否符合業務須知（Need-to-Know）與執行工作所需合理權限原則？	☐ 不適用	
	7.12 是否針對機關（單位）同仁及外部人員（如：合作機關（構）、廠商、工讀生等）配賦唯一的使用者識別碼並具備合適的身分鑑別措施？是否建立適當之複核機制？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.13 人員離職或職務異動時，是否由原屬權責主管審查存取授權之異動？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.14 如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.15 以電子郵件傳送敏感級以上個資檔案時，是否採加密機制，並確認加密機制之有效性？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.16 存放個人資料檔案之電腦是否定期執行各項漏洞修補程式或安全性更新？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.17 存放個人資料檔案之電腦是否全面使用防毒軟體並即時更新病毒碼？	☐ 符合 ☐ 不符合 ☐ 不適用	
	7.18 存放個人資料檔案之電腦設備委外維修或報廢時，是否事先移除個人資料？	☐ 符合 ☐ 不符合 ☐ 不適用	

附件二十八：個人資料安全稽核檢查表（第3版）

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	7.19 存放個人資料檔案之電腦設備攜出或借出時，是否經權責主管授權核准？	☐ 符合 ☐ 不符合 ☐ 不適用	
8.個人資料使用紀錄、軌跡資料及相關證據應妥善保管、定期覆核	8.1 是否對保存之個資進行紀錄（如存取及利用紀錄、調閱紀錄、軌跡資料）、證據之管理措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.2 是否定有保管期限？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.3 延長保管期限時，是否依照規定？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.4 是否依保管期限確實刪除或銷毀？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.5 因業務需求經權責主管授權執行個人資料之處理行為，是否留存包括使用者身分與其行為內容等之使用紀錄或軌跡資料以供事後查核或舉證？	☐ 符合 ☐ 不符合 ☐ 不適用	
	8.6 權責主管或管理人員，是否定期審查相關使用紀錄或軌跡資料？	☐ 符合 ☐ 不符合 ☐ 不適用	
9.委外作業	9.1 是否有委外蒐集、處理或利用個人資料之情形並簽訂書面契約？	☐ 符合 ☐ 不符合 ☐ 不適用	當年度無委外作業者，9.1-9.5 應填不適用
	9.2 是否將受託者之個人資料安全維護措施列入評選項目？	☐ 符合 ☐ 不符合 ☐ 不適用	
	9.3 是否定期確認受託者執行狀況，並作成紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	
	9.4 提出限期改善時，是否持續追蹤改善情形？	☐ 符合 ☐ 不符合 ☐ 不適用	

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	9.5 契約終止或解除時，是否要求受託者確實刪除、銷毀或返還？	☐ 符合 ☐ 不符合 ☐ 不適用	
10. 資料安全稽核機制	10.1 是否訂定定期檢視各項個人資料保護措施之資料安全稽核作業機制？	☐ 符合 ☐ 不符合 ☐ 不適用	
	10.2 稽核作業結束後，是否將稽核結果製作報告備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	10.3 是否針對稽核結果進行後續改正作業，並保留矯正作業執行紀錄？	☐ 符合 ☐ 不符合 ☐ 不適用	
11. 缺失改善與矯正預防作業	11.1 是否訂定矯正及預防程序，於各類查核發現不符合、觀察或建議事項時，進行根因分析，並採取適當之矯正及預防措施？	☐ 符合 ☐ 不符合 ☐ 不適用	
	11.2 是否對各類查核發現之不符合事項之矯正與預防措施訂定合理之執行期限且追蹤執行結果，並有相關紀錄備查？	☐ 符合 ☐ 不符合 ☐ 不適用	
	11.3 針對各類查核發現之不符合事項矯正措施，是否於執行期限內完成？是否持續追蹤至改善完成？	☐ 符合 ☐ 不符合 ☐ 不適用	
12. 配合嚴重特殊傳染性肺炎中央流行疫情指揮中心之要求	12.1 於 COVID-19 期間執行防疫措施蒐集之個人資料，是否依規定蒐集？有無蒐集必要？	☐ 符合 ☐ 不符合 ☐ 不適用	無執行防疫措施，或執行之防疫措施不會蒐集到個人資料者，12.1-12.3 應填不適用
	12.2 是否指派專人保管？電子個人資料是否加密儲存？	☐ 符合 ☐ 不符合 ☐ 不適用	
	12.3 是否依預定刪除時間及刪	☐ 符合 ☐ 不符合	

稽核項目	稽核內容（得視情形增刪）	稽核結果	說明
	除方式，刪除所保存之個人資料？	☐ 不適用	
13.對非公務機關個人資料保護之監管	13.1 是否定期檢討依個資法第27條第3項訂定相關辦法之必要性？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明依 <u>行政院及所屬各機關落實個人資料保護聯繫作業要點第5點</u> 所列情形綜合考量之檢討結果。 已訂定相關辦法或無監管非公務機關者，應填不適用。
	13.2 已訂定相關辦法者，就該辦法所規定之事項，是否完整？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明是否依前揭作業要點訂定。 未訂定相關辦法者，應填不適用。
	13.3 是否檢視個資法第22條第1項規定之情形，採取行政檢查？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明檢視之結果。 無監管非公務機關者，應填不適用。
	13.4 採取行政檢查時，是否符合個資法第22條至第24條之規定？	☐ 符合 ☐ 不符合 ☐ 不適用	請檢附實施檢查之紀錄。 未採取行政檢查者，應填不適用。
	13.5 非公務機關有違反個資法規定之情事者，進行處分時是否符合個資法第25條之規定？	☐ 符合 ☐ 不符合 ☐ 不適用	請檢附處分書。 未採取處分者，應填不適用。
	13.6 公布非公務機關之違法情形及其姓名或名稱與負責人時，是否妥善考量相關因素？	☐ 符合 ☐ 不符合 ☐ 不適用	請說明公布之方式並檢附公布內容。 未公布者，應填不適用。