

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
三、 <u>(刪除)</u>	<p>三、本作業程序不適用個人資料保護法（以下簡稱本法）施行細則所定個人資料去識別化作業。</p> <p>含個人資料檔案於非法定業務或當事人同意之目的外利用前（例如編輯成開放資料供統計等用途），應依本局「IMP-800-001 個人資料去識別作業規範」執行去識別化，確認檔案內之個人資料無法再識別後，方得使用。</p>	<p>一、<u>本點刪除。</u></p> <p>二、內容已整併至第十三點有關特定目的外利用之規定，爰予刪除。</p>
<p>十三、個人資料之利用，應依下列程序辦理：</p> <p>（一）利用個人資料時，應於法定職務之必要範圍內並與蒐集之特定目的相符。</p> <p>（二）不得非法利用個人資料，並不得為資料庫之恣意連結，且不得濫用。</p> <p>（三）以本法第十五條第二款「經當事人同意」方式蒐集個人資料時，對於個人資料之利用應符合該同意書所載之內容，包括個人資料利用之期間、地區、對象、方式及其他相關事項。</p> <p>（四）特定目的外之利用：</p> <p>1. 對於個人資料之利用，如有特定目的外利用之情況，應符合下列情形之一：</p> <p>（1）法律明文規定。</p> <p>（2）為維護國家安全或增進公共利益所必要。</p> <p>（3）為免除當事人之生命、身體、自由或財產上之危險。</p>	<p>十三、個人資料之利用，應依下列程序辦理：</p> <p>（一）利用個人資料時，應於法定職務之必要範圍內並與蒐集之特定目的相符。</p> <p>（二）不得非法利用個人資料，並不得為資料庫之恣意連結，且不得濫用。</p> <p>（三）以本法第十五條第二款「經當事人同意」方式蒐集個人資料時，對於個人資料之利用應符合該同意書所載之內容，包括個人資料利用之期間、地區、對象、方式及其他相關事項。</p> <p>（四）特定目的外之利用：</p> <p>1. 對於個人資料之利用，如有特定目的外利用之情況，應符合下列情形之一：</p> <p>（1）法律明文規定。</p> <p>（2）為維護國家安全或增進公共利益所必要。</p> <p>（3）為免除當事人之生命、身體、自由或財產上之危險。</p> <p>（4）為防止他人權益之重</p>	<p>配合本局「IMP-800-001 個人資料去識別作業規範」文件廢止，另為整併現行規定第三點有關個人資料執行去識別化技術之運用，爰增訂第四款第五目。</p>

<p>(4)為防止他人權益之重大危害。</p> <p>(5)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經蒐集者依其揭露方式無從識別特定之當事人。</p> <p>(6)有利於當事人權益。</p> <p>(7)經當事人同意。</p> <p>2. 對保有之個人資料有特定目的外利用之需求時，個人資料之利用單位應詳為審核，填具「個人資料檔案特定目的外利用查檢表」(附件六)，簽奉核定後為之。</p> <p>3. 以本法第十六條但書第七款「經當事人同意」之方式對保有之個人資料為特定目的外利用時，應備妥「個人資料特定目的外利用同意書」(附件七)，以取得當事人同意。</p> <p>4. 依本法第十六條但書規定對個人資料為特定目的外之利用，個人資料之利用單位應將個人資料之利用歷程做成紀錄。</p> <p>5. <u>含個人資料檔案於非法定業務或當事人同意之目的外利用前(例如編輯成開放資料供統計等用途)，得參考 CNS 20889「隱私增強資料去識別化術語與技術分類」執行去識別化，確認檔案內之個人資料無法再識別後，方得使用。</u></p> <p>(五) 個人資料檔案之利用，於不顯示當事人個人資料明細時，宜遵循「個人資料隱碼規則」(附件八)，對所利用之個人資料進行遮罩，以保護當事人之</p>	<p>大危害。</p> <p>(5)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經蒐集者依其揭露方式無從識別特定之當事人。</p> <p>(6)有利於當事人權益。</p> <p>(7)經當事人同意。</p> <p>2. 對保有之個人資料有特定目的外利用之需求時，個人資料之利用單位應詳為審核，填具「個人資料檔案特定目的外利用查檢表」(附件六)，簽奉核定後為之。</p> <p>3. 以本法第十六條但書第七款「經當事人同意」之方式對保有之個人資料為特定目的外利用時，應備妥「個人資料特定目的外利用同意書」(附件七)，以取得當事人同意。</p> <p>4. 依本法第十六條但書規定對個人資料為特定目的外之利用，個人資料之利用單位應將個人資料之利用歷程做成紀錄。</p> <p>(五) 個人資料檔案之利用，於不顯示當事人個人資料明細時，宜遵循「個人資料隱碼規則」(附件八)，對所利用之個人資料進行遮罩，以保護當事人之資料隱私。</p> <p>(六) 已歸檔不再利用之來自第三方之個人資料，首次再利用時，準用第十點規定辦理。</p>	
--	--	--

<p>資料隱私。</p> <p>(六)已歸檔不再利用之來自第三方之個人資料，首次再利用時，準用第十點規定辦理。</p>		
<p>二十九、個人資料風險評估作業，依下列程序辦理：</p> <p>(一)本局及各分局之個人資料檔案，依本局「IM3-01-01 資訊安全風險評鑑程序書」，併同每年度資訊安全風險重新評鑑作業進行：</p> <ol style="list-style-type: none"> 1. 由資料蒐集單位負責將個人資料檔案列入風險評鑑資訊資產清冊中。 2. 本小組行政組依據本局個人資料隱私保護要求，維護「個人資料類別隱私衝擊分級表」(附件十五)，將資料類別依對當事人之隱私衝擊進行分級。 3. 進行風險評估時，其風險水準應保持與個人資料類別之隱私衝擊對應。 4. 進行風險評估時，除評估屬紙本文件或電子文件之資訊安全風險外，尚需針對紙本個人資料及電子個人資料之風險進行評估。 <p>(二)各單位識別出屬個人資料檔案之巨高風險者，應通知本小組行政組，規劃適當之管控機制。其屬中低風險者，由各單位自行管控以預防個人資料檔案遭受竊取、竄改、毀損、滅失或洩漏等風險之發生。</p> <p>(三)其他相關作業事項及應使用之表單，依本局每年度資訊安全風險重新評鑑作業計畫辦理。</p>	<p>二十九、個人資料風險評估作業，依下列程序辦理：</p> <p>(一)本局及各分局之個人資料檔案，依本局「IMP-000-001 資訊安全風險評鑑程序書」，併同每年度資訊安全風險重新評鑑作業進行：</p> <ol style="list-style-type: none"> 1. 由資料蒐集單位負責將個人資料檔案列入風險評鑑資訊資產清冊中。 2. 本小組行政組依據本局個人資料隱私保護要求，維護「個人資料類別隱私衝擊分級表」(附件十五)，將資料類別依對當事人之隱私衝擊進行分級。 3. 進行風險評估時，其風險水準應保持與個人資料類別之隱私衝擊對應。 4. 進行風險評估時，除評估屬紙本文件或電子文件之資訊安全風險外，尚需針對紙本個人資料及電子個人資料之風險進行評估。 <p>(二)各單位識別出屬個人資料檔案之巨高風險者，應通知本小組行政組，規劃適當之管控機制。其屬中低風險者，由各單位自行管控以預防個人資料檔案遭受竊取、竄改、毀損、滅失或洩漏等風險之發生。</p> <p>(三)其他相關作業事項及應使用之表單，依本局每年度資訊安全風險重新評鑑作業計畫辦理。</p>	<p>現行規定第一款本文配合本局「IMP-000-001 資訊安全風險評鑑程序書」文件改版，爰予修正。</p>
<p>三十一、事故通報之作業程序：</p> <p>(一)個人資料安全事故，指以</p>	<p>三十一、事故通報之作業程序：</p> <p>(一)個人資料安全事故，指以</p>	<p>現行規定第二款第二目之二配合「</p>

<p>下二種類型之事件：</p> <ol style="list-style-type: none"> 1. 任何個人資料被竊取、竄改、毀損、滅失或洩漏之事件，足以損害當事人權益者。 2. 其他有相關或牽連之事件，足以損害當事人權益者。 <p>(二) 內部通報流程：</p> <ol style="list-style-type: none"> 1. 凡發現可能導致個人資料安全事故之事件時，應立即通報所屬單位或分局之個人資料保護聯絡人員、專責人員、資訊安全官及本小組行政組，共同分析事件狀況，判定是否為第一款所定之事件，並由聯絡人員及本小組行政組，將處理過程記錄於「個人資料安全事件通報單」(附件十六)。 2. 事件經確認為個人資料安全事故者，應執行下列作業： <ol style="list-style-type: none"> (1) 由本小組行政組通報至本局資訊安全長、主任秘書、法務室主任及資訊室主任。 (2) 發生個人資料安全事故之單位或分局個人資料保護專責人員，並應通報單位主管或分局長，屬電子資料之資安事件者，應同時依「<u>經濟部標準檢驗局資通安全事件通報及應變處理作業程序</u>」辦理通報等規定之作業。 (3) 依第三十二點執行事故應變作業程序。 3. 「個人資料安全事件通報單」(附件十六)核定後，由本小組行政組歸檔備 	<p>下二種類型之事件：</p> <ol style="list-style-type: none"> 1. 任何個人資料被竊取、竄改、毀損、滅失或洩漏之事件，足以損害當事人權益者。 2. 其他有相關或牽連之事件，足以損害當事人權益者。 <p>(二) 內部通報流程：</p> <ol style="list-style-type: none"> 1. 凡發現可能導致個人資料安全事故之事件時，應立即通報所屬單位或分局之個人資料保護聯絡人員、專責人員、資訊安全官及本小組行政組，共同分析事件狀況，判定是否為第一款所定之事件，並由聯絡人員及本小組行政組，將處理過程記錄於「個人資料安全事件通報單」(附件十六)。 2. 事件經確認為個人資料安全事故者，應執行下列作業： <ol style="list-style-type: none"> (1) 由本小組行政組通報至本局資訊安全長、主任秘書、法務室主任及資訊室主任。 (2) 發生個人資料安全事故之單位或分局個人資料保護專責人員，並應通報單位主管或分局長，屬電子資料之資安事件者，應同時依「IMP-000-212 資通安全事件/故管理作業規範」辦理通報等規定之作業。 (3) 依第三十二點執行事故應變作業程序。 3. 「個人資料安全事件通報單」(附件十六)核定後，由本小組行政組歸檔備查。 <p>(三) 外部通報流程：通報經</p>	<p>IMP-000-212 資通安全事件/故管理作業規範」改訂為「經濟部標準檢驗局資通安全事件通報及應變處理作業程序」，爰予修正。</p>
--	--	--

<p>查。</p> <p>(三) 外部通報流程：通報經濟部個人資料保護推動執行小組（以下簡稱本部個資小組）</p> <p>1. 事件經確認為個人資料安全事故者，本小組行政組主辦單位人員應立即依「經濟部個人資料保護作業手冊」之規定，通報本部個資小組。</p> <p>2. 如個人資料安全事故涉及資通安全面，本小組資訊組應另依其資通安全事件通報及應變機制至行政院國家資通安全通報應變網站進行通報。</p> <p>(四) 通報應以電話、傳真或任何可資運用之即時通知、溝通工具迅速傳達之。</p> <p>(五) 發生個人資料安全事故之事件時，應自發現時起，保存調查、分析、處理、補救措施、通報、通知及其事後相關處理之歷程紀錄及相關證據，超過本法第三十條規定當事人損害賠償請求權消滅時效者，始得銷燬或刪除。但應保存事件摘要文件，以利證明當事人損害賠償請求權消滅時效之起算及屆滿時點。</p>	<p>濟部個人資料保護推動執行小組（以下簡稱本部個資小組）</p> <p>1. 事件經確認為個人資料安全事故者，本小組行政組主辦單位人員應立即依「經濟部個人資料保護作業手冊」之規定，通報本部個資小組。</p> <p>2. 如個人資料安全事故涉及資通安全面，本小組資訊組應另依其資通安全事件通報及應變機制至行政院國家資通安全通報應變網站進行通報。</p> <p>(四) 通報應以電話、傳真或任何可資運用之即時通知、溝通工具迅速傳達之。</p> <p>(五) 發生個人資料安全事故之事件時，應自發現時起，保存調查、分析、處理、補救措施、通報、通知及其事後相關處理之歷程紀錄及相關證據，超過本法第三十條規定當事人損害賠償請求權消滅時效者，始得銷燬或刪除。但應保存事件摘要文件，以利證明當事人損害賠償請求權消滅時效之起算及屆滿時點。</p>	
<p>三十六、個人資料安全事故處理報告於核定後，本小組行政組應依據核定之改善方案，請應改善單位依據「IM3-01-03 資訊安全管理系統矯正程序書」辦理，並列管追蹤其執行及改善有效性。</p>	<p>三十六、個人資料安全事故處理報告於核定後，本小組行政組應依據核定之改善方案，請應改善單位依據「IMP-000-006 資訊安全管理系統矯正程序書」辦理，並列管追蹤其執行及改善有效性。</p>	<p>配合本局「IMP-000-006 資訊安全管理系統矯正程序書」文件改版，爰予修正。</p>

<p>四十五、個人資料電子文書檔案之安全維護注意事項：</p> <p>(一) 個人資料電子文書檔案係指以商用軟體對個人資料進行文書處理後所儲存之檔案（例如將傳真報名活動人員以 Microsoft Excel 軟體處理後儲存之電子檔案）。</p> <p>(二) 含有個人資料之電子文書檔案儲存或傳遞時，應以加密軟體加密保護。加密保護相關作業，依「<u>IM2-02-01 資訊處理設施之資訊安全作業規範</u>」辦理。</p> <p>(三) 設定密碼之個人資料電子文書檔案密碼應予造冊（附件二十），清冊依「<u>IM2-02-01 資訊處理設施之資訊安全作業規範</u>」保護。承辦人設定密碼時，應採用安全強度足夠之密碼，工作變更時列入移交，取得他人移交之加密電子檔案後應變更加密密碼。</p> <p>(四) 個人資料電子文書檔案之備份由該檔案承辦人負責，原始檔案及備份檔案位置皆應紀錄於「個人資料電子文書檔案密碼清冊」（附件二十）中。</p> <p>(五) 個人資料電子文書檔案，應避免以電子郵件傳遞，若以電子郵件傳遞時，讀取密碼應與檔案以不同之電子郵件分開傳送。對外部機關構傳送個人資料檔案時應確定該傳送在原個人資料檔案之可利用範圍內，並且已先行告知當事人該傳送之對象及方式。</p>	<p>四十五、個人資料電子文書檔案之安全維護注意事項：</p> <p>(一) 個人資料電子文書檔案係指以商用軟體對個人資料進行文書處理後所儲存之檔案（例如將傳真報名活動人員以 Microsoft Excel 軟體處理後儲存之電子檔案）。</p> <p>(二) 含有個人資料之電子文書檔案儲存或傳遞時，應以加密軟體加密保護。加密保護相關作業，依「<u>IMP-000-204 資訊資產之資訊安全作業規範</u>」第 6.2 節規定辦理。</p> <p>(三) 設定密碼之個人資料電子文書檔案密碼應予造冊（附件二十），清冊依「<u>IMP-000-204 資訊資產之資訊安全作業規範</u>」第 6.2 節規定保護。承辦人設定密碼時，應採用安全強度足夠之密碼，工作變更時列入移交，取得他人移交之加密電子檔案後應變更加密密碼。</p> <p>(四) 個人資料電子文書檔案之備份由該檔案承辦人負責，原始檔案及備份檔案位置皆應紀錄於「個人資料電子文書檔案密碼清冊」（附件二十）中。</p> <p>(五) 個人資料電子文書檔案，應避免以電子郵件傳遞，若以電子郵件傳遞時，讀取密碼應與檔案以不同之電子郵件分開傳送。對外部機關構傳送個人資料檔案時應確定該傳送在原個人資料檔案之可利用範圍內，並且已先行告知當事人該傳送之對象及方式。</p>	<p>現行規定第二款及第三款配合本局「IMP-000-204 資訊資產之資訊安全作業規範」文件改版，爰予修正。</p>
---	---	---

<p>四十六、個人資料利用應用系統蒐集處理與利用之安全維護注意事項：</p> <p>(一) 網際網路防護之安全：保有個人資料之伺服器連接網際網路，應遵循「<u>IM2-06-02 網路通訊之資訊安全作業規範</u>」辦理。</p> <p>(二) 電腦系統之安全：所有蒐集、處理或利用個人資料之電腦設備及使用使用者，應遵循「<u>IM2-06-01 系統運作之資訊安全作業規範</u>」防範惡意軟體之規定。</p> <p>(三) 個人資料資料庫之安全：</p> <ol style="list-style-type: none"> 1. 用以蒐集、處理或利用個人資料之應用系統，應明定安全需求，訂定時應遵循「<u>IM2-07-01 應用資通系統之資訊安全作業規範</u>」。 2. 蒐集、處理或利用個人資料之資料庫，資料保存單位應評估資料內容之敏感程度及資料數量，遵循「<u>IM2-06-01 系統運作之資訊安全作業規範</u>」。 <p>(四) 存取控制：存取電子個人資料檔案，應遵循「<u>IM2-09-01 識別與存取控制作業規範</u>」。</p> <p>(五) 實體場地及設施設備安全：</p> <ol style="list-style-type: none"> 1. 場所安全： <ol style="list-style-type: none"> (1) 處理個人資料之辦公場所，無人留守或下班時，均應鎖閉。 (2) 處理個人資料之電腦設備集中區域及 	<p>四十六、個人資料利用應用系統蒐集處理與利用之安全維護注意事項：</p> <p>(一) 網際網路防護之安全：保有個人資料之伺服器連接網際網路，應遵循「<u>IMP-000-209 資料通訊之資訊安全作業規範</u>」第 6 節相關規定辦理。</p> <p>(二) 電腦系統之安全：所有蒐集、處理或利用個人資料之電腦設備及使用使用者，應遵循「<u>IMP-000-208 系統運作之資訊安全作業規範</u>」第 6.6 節防範惡意軟體之規定。</p> <p>(三) 個人資料資料庫之安全：</p> <ol style="list-style-type: none"> 1. 用以蒐集、處理或利用個人資料之應用系統，應明定安全需求，訂定時應遵循「<u>IMP-000-210 系統採購開發及維護之資訊安全作業規範</u>」第 6 節規定辦理。 2. 蒐集、處理或利用個人資料之資料庫，資料保存單位應評估資料內容之敏感程度及資料數量，遵循「<u>IMP-000-208 系統運作之資訊安全作業規範</u>」第 6.2 節及第 6.3 節等規定辦理。 <p>(四) 存取控制：存取電子個人資料檔案，應遵循「<u>IMP-000-205 存取控制作業規範</u>」第 6.6 節規定辦理。</p> <p>(五) 實體場地及設施設備安全：</p> <ol style="list-style-type: none"> 1. 場所安全： <ol style="list-style-type: none"> (1) 處理個人資料之辦公場所，無人留守或下班時，均應鎖閉。 (2) 處理個人資料之電腦 	<p>現行規定第一款至第四款配合本局資訊安全管理系統(ISMS)文件改版，爰予修正。</p>
--	---	--

<p>檔案儲存區域，應設立進出管制。高度集中區域，如機房及檔案室，應規劃空調、偵煙、偵熱及滅火設備。電腦設備，應採「氣體式滅火器」。</p> <p>(3)處理個人資料之儲存媒體及設備有報廢之必要者，應於報廢前，先行評估有無任何敏感資料或個人資料，並先行確保所有敏感資料或個人資料均確實刪除、覆寫或進行破壞。</p> <p>2. 桌面淨空及螢幕淨空：</p> <p>(1)處理個人資料之人員暫時離開座位時，應將其所經辦或使用具有個人資料文件（例如：公文、報名及會員資料等）及資料儲存媒體（例如：USB 隨身碟、磁碟片及光碟等）妥善存放，且不得置於個人電腦桌面。</p> <p>(2)處理個人資料之人員長時離開座位者，應登出個人資料處理系統、鎖定電腦或啟動電腦螢幕保護，或關閉個人電腦。</p> <p>3. 工作場所外作業：</p> <p>(1)單位主管應核定「個人資料檔案禁止攜出清冊」（附件二十一），明定禁止攜出工作場所外之敏感性個人資料檔案項目，確實要求作業人員遵循。</p> <p>(2)攜出工作場所外之</p>	<p>設備集中區域及檔案儲存區域，應設立進出管制。高度集中區域，如機房及檔案室，應規劃空調、偵煙、偵熱及滅火設備。電腦設備，應採「氣體式滅火器」。</p> <p>(3)處理個人資料之儲存媒體及設備有報廢之必要者，應於報廢前，先行評估有無任何敏感資料或個人資料，並先行確保所有敏感資料或個人資料均確實刪除、覆寫或進行破壞。</p> <p>2. 桌面淨空及螢幕淨空：</p> <p>(1)處理個人資料之人員暫時離開座位時，應將其所經辦或使用具有個人資料文件（例如：公文、報名及會員資料等）及資料儲存媒體（例如：USB 隨身碟、磁碟片及光碟等）妥善存放，且不得置於個人電腦桌面。</p> <p>(2)處理個人資料之人員長時離開座位者，應登出個人資料處理系統、鎖定電腦或啟動電腦螢幕保護，或關閉個人電腦。</p> <p>3. 工作場所外作業：</p> <p>(1)單位主管應核定「個人資料檔案禁止攜出清冊」（附件二十一），明定禁止攜出工作場所外之敏感性個人資料檔案項目，確實要求作業人員遵循。</p> <p>(2)攜出工作場所外之處</p>	
--	--	--

<p>處理個人資料設備，應設有讀取密碼，成本允許下應採用資料加密措施，以免攜出設備遺失或遭竊後，個人資料檔案內容遭不當利用。</p> <p>(3)於工作場所外，不得以指定設備以外之其他設備，處理個人資料檔案。</p> <p>(4)攜出處理個人資料檔案之設備，不得使用無線網路服務。</p>	<p>理個人資料設備，應設有讀取密碼，成本允許下應採用資料加密措施，以免攜出設備遺失或遭竊後，個人資料檔案內容遭不當利用。</p> <p>(3)於工作場所外，不得以指定設備以外之其他設備，處理個人資料檔案。</p> <p>(4)攜出處理個人資料檔案之設備，不得使用無線網路服務。</p>	
<p>五十七、個人資料委外監督作業程序及相關事項，依本章規定辦理，本章未規定者，依「<u>IM2-12-01 資訊處理供應鏈之資訊安全作業規範</u>」辦理。</p>	<p>五十七、個人資料委外監督作業程序及相關事項，依本章規定辦理，本章未規定者，依「IMW-000-004 委外作業資訊安全與隱私保護管理規定」辦理。</p>	<p>配合本局「IMW-000-004 委外作業資訊安全與隱私保護管理規定」文件改版，爰予修正。</p>
<p>六十、個人資料檔案安全稽核結果之缺失改善、追蹤及矯正預防等作業，依「<u>IM3-01-02 資訊安全管理系統稽核程序書</u>」、「<u>IM3-01-03 資訊安全管理系統矯正程序書</u>」及「IM1 資訊安全管理手冊」等相關規定辦理。</p>	<p>六十、個人資料檔案安全稽核結果之缺失改善、追蹤及矯正預防等作業，依「IMP-000-015 資訊安全管理系統稽核程序書」、「IMP-000-006 資訊安全管理系統矯正程序書」及「IM1 資訊安全管理手冊」等相關規定辦理。</p>	<p>配合本局「IMP-000-015 資訊安全管理系統稽核程序書」、「IMP-000-006 資訊安全管理系統矯正程序書」文件改版，爰予修正。</p>

經濟部標準檢驗局（○○分局） 個人資料檔案特定目的外利用查檢表			
簽核	承辦人	科(課)長	批示
保有個人資料檔案 名稱			
利用單位			
個人資料類別 （請填資料項目）			
個人資料類別代碼			
辦理方式	<input type="checkbox"/> 本局自行辦理 <input type="checkbox"/> 委外辦理（契約要求_____）		
個人資料 敏感程度	個人資料類別隱私衝擊分級之最高級： <input type="checkbox"/> 3 <input type="checkbox"/> 2 <input type="checkbox"/> 1 【請參閱附件十五：個人資料類別隱私衝擊分級表】		
現行利用目的			
現行利用目的代碼			
目的外利用目的			
目的外利用目的 代碼			
目的外利用依據	<input type="checkbox"/> 法律明文規定：_____ <input type="checkbox"/> 為維護國家安全或增進公共利益所必要： _____ <input type="checkbox"/> 為免除當事人之生命、身體、自由或財產上之危險： _____ <input type="checkbox"/> 為防止他人權益之重大危害： _____ <input type="checkbox"/> 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經蒐集者依其揭露方式無從識別特定之當事人： _____		

附件六：個人資料檔案特定目的外利用查檢表（第1版）（本附件未修正）

	<p><input type="checkbox"/>有利於當事人權益：</p> <p>_____</p> <p><input type="checkbox"/>經當事人同意</p> <p><input type="checkbox"/>書面同意（同意書如附件_____）</p> <p><input type="checkbox"/>電子文件採用之舉證方式</p> <p><input type="checkbox"/>電子簽章（方法_____）</p> <p><input type="checkbox"/>數位簽章（方法_____）</p> <p><input type="checkbox"/>其他</p>
採當事人同意之告知事項	<p>查檢項目</p> <p><input type="checkbox"/>特定目的外之其他利用目的。</p> <p><input type="checkbox"/>利用之範圍（機關/組織、地區、時間）。</p> <p><input type="checkbox"/>同意與否對其權益之影響。</p> <p><input type="checkbox"/>有多項之利用目的時，是否單獨列出。</p>
個人資料檔案安全維護	<p><input type="checkbox"/>紙本</p> <p><input type="checkbox"/>由當事人（或其指定代理人）直接至本局交付</p> <p><input type="checkbox"/>由當事人（或其指定代理人）透過第三方傳遞至本局</p> <p><input type="checkbox"/>由本局於局外蒐集（蒐集地點_____）</p> <p><input type="checkbox"/>由本局委託單位於室內蒐集（蒐集地點_____）</p> <p><input type="checkbox"/>由本局委託單位於戶外蒐集（蒐集地點_____）</p> <p><input type="checkbox"/>由第三方取得提供</p> <p><input type="checkbox"/>第三方已取得當事人同意交付本局</p> <p><input type="checkbox"/>本局使用前需告知當事人（告知事項如附件_____）</p> <p>檔案保護方式_____</p> <p><input type="checkbox"/>電子</p> <p><input type="checkbox"/>由當事人或指定代理人</p> <p><input type="checkbox"/>自行輸入系統 <input type="checkbox"/>提供電子媒體</p> <p><input type="checkbox"/>由紙本蒐集後輸入應用系統</p> <p>資料庫伺服器位置：<input type="checkbox"/>本局 <input type="checkbox"/>其他_____</p> <p>檔案保護方式_____</p> <p><input type="checkbox"/>共用應用系統。提供機關_____</p> <p><input type="checkbox"/>由紙本蒐集後製成電子檔案 <input type="checkbox"/>由資訊系統再轉存至電子檔案</p> <p>檔案保護方式_____</p>

附件六：個人資料檔案特定目的外利用查檢表（第1版）（本附件未修正）

紙本資料風險評估	估算風險值＝															
	低風險				中風險				高風險				巨風險			
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	風險發生後可能影響之最高個人資料筆數估算 <input type="checkbox"/> 5：5001（含）筆以上 <input type="checkbox"/> 4：2000-5000（含）筆 <input type="checkbox"/> 3：1000-2000（含）筆 <input type="checkbox"/> 2：501-1000（含）筆 <input type="checkbox"/> 1：1-500（含）筆															
	風險值＝個人資料敏感程度 x（有可能發生風險數 / 12）x 可能影響之資料數量															
	風險情形											風險發生				
												有可能		幾無可能		
	1.個人資料在蒐集時缺乏嚴謹資料保護，而造成遺失或未授權人員竊取、複製、洩露、竄改或損毀。															
	2.個人資料因保存缺乏嚴謹資料保護，而造成資料減失或未授權人員竊取、複製、洩露、竄改或損毀。															
	3.個人資料因缺乏文件存取管制，而造成個人資料之違反法律之處理或利用。															
	4.個人資料因授權存取人員瀆職，而造成授權人員的複製、洩露、竄改或刪除。															
	5.個人資料因未監督外來人員或清潔人員之工作，而造成個人資料遭竊取、複製或損毀。															
	6.個人資料因人員缺乏安全的認知(awareness)，而造成內部人員複製、揭露。															
	7.個人資料因文件廢棄處理不安全，而造成未授權人員複製、揭露。															
	8.個人資料因紙張再利用沒有排除有個資的資料，而造成未授權人員複製、揭露。															
9.個人資料因人員缺乏正確的法規認知而造成違反法規的資料比對、處理或利用。																
10.個人資料因未適當規範監督委外廠商，而造成委外廠商人員故意或疏忽，資料被違法蒐集、處理、利用或遭竊取、複製、洩露、竄改或損毀。																
11.個人資料因人員紀律不足，沒有依標準規範作業，而造成資料的外洩、錯誤或損毀。																
12.個人資料因未保留管理紀錄，而造成無法提出舉證資料。																

附件六：個人資料檔案特定目的外利用查檢表（第1版）（本附件未修正）

電子資料風險評估	估算風險值＝															
	低風險				中風險				高風險				巨風險			
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	風險發生後可能影響之最高個人資料筆數估算 <input type="checkbox"/> 5：5001（含）筆以上 <input type="checkbox"/> 4：2000-5000（含）筆 <input type="checkbox"/> 3：1000-2000（含）筆 <input type="checkbox"/> 2：501-1000（含）筆 <input type="checkbox"/> 1：1-500（含）筆															
	風險值＝個人資料敏感程度 x（有可能發生風險數 / 12）x 可能影響之資料數量															
	風險情形											風險發生				
												有可能		幾無可能		
	1.個人資料因傳輸資料未加讀取密碼或網路傳輸時沒有加密處理，而造成資料外洩。															
	2.個人資料因設備不安全（含無密碼存取控制、未設定安全、未實施安全防護如防毒或軟體修補），而造成資料被複製揭露、被竄改或刪除。															
	3.個人資料因應用系統不安全，而造成人為嘗試找出系統弱點，未授權存取複製揭露或竄改。															
	4.個人資料因存放個資的伺服器或電腦供匿名存取，或多人共用帳號密碼而造成資料被複製揭露、被竄改或刪除，且無法找出是誰所為。															
	5.個人資料因電子資料檔案（儲存媒體）被攜出，而造成遺失被外部人員複製揭露。															
	6.個人資料因電子資料檔案（儲存媒體）缺乏嚴謹資料保護，而造成未授權人員複製揭露、竊取或損毀。															
	7.個人資料因沒有備援存取機制，在意外發生後造成個人資料損毀，造成當事人權益受損。															
	8.個人資料因電子資料檔案（儲存媒體）廢棄或再利用不安全，而造成未授權人員複製揭露。															
9.個人資料因人員缺乏正確的法規認知而造成違反法規的資料串連、比對、利用與傳遞。																
10.個人資料因未適當規範監督委外廠商，而造成委外廠商設備不安全或人員故意或疏忽，資料被複製揭露或被竄改或損失。																
11.個人資料因人員紀律不足，沒有依標準規範作業，或授權存取者瀆職而造成授權人員的複製揭露、竄改或刪除。																
12.個人資料因依法刪除時沒有保留紀錄而造成無法提出舉證資料。																

填表說明

欄位	說明
保有個人資料檔案名稱	預定為特定目的外利用之個人資料檔案於「個人資料檔案彙整表」（附件十二）所登載之個人資料檔案名稱。
利用單位	預定為特定目的外利用之單位。
個人資料類別	預定為特定目的外利用之個人資料檔案於「個人資料檔案彙整表」（附件十二）所登載之個人資料類別。
個人資料類別代碼	預定為特定目的外利用之個人資料檔案於「個人資料檔案彙整表」（附件十二）所登載之個人資料類別代碼。
辦理方式	勾選方式，若採用委外辦理時，應標註個人資料保護條款納入委外契約條款之條、項或款次。（例如契約草案第20條個人資料檔案安全維護管理。）
個人資料敏感程度	依預定為特定目的外利用之個人資料檔案項目之分類，勾選相對的敏感程度類別。敏感程度愈高，對於個人資料檔案的維護水準亦應相對提高。
現行利用目的	以文字說明現行利用目的，請填寫利用到個人資料的所有作業。
現行利用目的代碼	依據現行個人資料利用目的，填寫其對應「個人資料保護法之特定目的及個人資料之類別」之特定目的代碼。例如一〇九教育或訓練行政（訓練報名、旅遊平安保險及發給證書）。
目的外利用目的	以文字說明目的外利用目的，請填寫利用到個人資料的所有作業。
目的外利用目的代碼	依據目的外利用目的，填寫其對應「個人資料保護法之特定目的及個人資料之類別」之特定目的代碼。例如一〇九教育或訓練行政（訓練報名、旅遊平安保險及發給證書）。
目的外利用依據	勾選，並填入適當之說明。
採當事人同意之告知事項	勾選查檢項目，確保法定告知事項皆有納入。
個人資料檔案安全維護	勾選可能保有之個人資料檔案型式、途徑，並標示檔案保護方式之附件文件名稱及保護方式陳述之位置。個人資料檔案之保護應兼顧個人資料之敏感程度及曝露之風險進行保護，以防止個人資料被竊取、洩漏、竄改或其他侵害。
風險評估	在「個人資料檔案安全維護」欄位評估之條件下，評估資料之資訊安全風險。若評估之風險值屬高風險或巨風險，應再增加個人資料檔案安全維護措施，修改「個人資料檔案安全維護」欄位之內容後，重新進行風險評估。

個人資料特定目的外利用同意書

為遵守個人資料保護法規定，並保障當事人之權利，謹依法告知下列事項：

1. 機關名稱：經濟部標準檢驗局（○○分局）
2. 原蒐集之特定目的：（例：國家經濟發展業務）（法務部公告之個人資料保護法之特定目的第一〇一項）¹
3. 其他利用之特定目的：（例：政令宣導）（法務部公告之個人資料保護法之特定目的第〇七二項）
4. 個人資料之類別²：（例：姓名、身分證編號、出生年月日、住址等）
5. 個人資料利用之期間、地區、對象及方式³：
 - (1) 期間：（例：蒐集後一年）
 - (2) 地區：（例：中華民國主權範圍內）
 - (3) 對象：（例：自行使用）
 - (4) 方式：（例：網站公告）
6. 依個人資料保護法第3條規定，當事人可行使以下權利⁴：
 - (1) 查詢或請求閱覽。
 - (2) 請求製給複製本。
 - (3) 請求補充或更正。
 - (4) 請求停止蒐集、處理及利用。
 - (5) 請求刪除。若有上述需求，請與本單位連繫，於填妥本單位當事人權利行使申請書後，本單位將依法進行回覆。另依個人資料保護法第14條規定，查詢或請求閱覽個人資料或製給複製本者，本單位得酌收必要成本費用。
7. 若您拒絕同意，本單位將無法提供您特定目的範圍外之相關服務⁵。

本人已充分知悉貴單位上述告知事項，並同意貴單位蒐集、處理、利用本人之個人資料。

立同意書人：

中華民國 年 月 日

-
1. 公務機關應於法定職務必要範圍內利用當事人之個人資料。請斟酌法定職務之內容，並參考法務部公告之特定目的項目表，填寫蒐集之特定目的。
 2. 個人資料之類別請參照法務部公告之個人資料類別表填寫。
 3. 個人資料之利用應於特定目的必要範圍內為之，特定目的範圍外之利用必須符合個人資料保護法第16條但書之要件，始為合法。另，特定目的之範圍將影響是否應該主動或依當事人請求為停止處理、利用及刪除之依據，本項請務必填寫完整。
 4. 當事人權利行使為個資法明定之當事人權利，請務必提供權利行使管道及方式。
 5. 若有其他對於當事人重要權益之影響，請務必於本項中一併告知。

機密等級：☒普通 ☐密 ☐機密 ☐極機密 ☐絕對機密
公開等級：☐主動公開 ☐公開 ☐限制公開 ☒不予公開

個人資料隱碼規則

資料項目	遮蔽規則	範例	備註
姓名	顯示第一字元 不論幾碼皆加○○	張菲 張○○ 歐陽菲菲 歐○○	或以** 取代○○
地址	顯示到鄉鎮區其後不論字 元數皆加*****	台北市大安區*****	或以○○○○○○ 取代*****
郵遞區號	僅顯示 3 碼	106	
電話號碼	隱藏後 4 碼	(02) 1234-**** 0935-12*****	
證號	隱藏後 4 碼	A12345****	得隱藏後 5 碼
電子郵件	前 4 碼, 不足補 e, 其後不 論字元數皆加****@（隱 藏第一區以***取代）	jaye*****@***. gov. tw	

機密等級：☒普通 ☐密 ☐機密 ☐極機密 ☐絕對機密
公開等級：☐主動公開 ☒公開 ☐限制公開 ☐不予公開

個人資料類別隱私衝擊分級表

個人資料隱私衝擊等級（依本局業務特性進行分級）：

1—普通資訊（一般當事人於社交活動中會願意提供，不會過於擔心隱私議題）

2—個人隱私資訊（一般當事人若非因特定目的通常不願意提供，提供時會擔心其隱私資料洩漏會有對個人不利的事件發生）

3—個人敏感隱私資訊（一般當事人希望保密的訊息，洩漏會有對個人極大的不利事件發生，或當事人心理感受傷害）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
識別類			
C001（1）	辨識個人者	例如：姓名、職稱、通訊地址、聯絡電話、電子郵遞地址。	1
C001（2）	辨識個人者	例如：以前地址、住址、工作地址、行動電話、住家電話號碼、戶籍地址、相片、即時通帳號、網路平臺申請之帳號、指紋、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。	2
C002	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。	2
C003	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。	2
特徵類			
C011	個人描述	例如：年齡、性別、出生年月日、出生地、國籍、聲音等。	2
C012	身體描述	例如：身高、體重、血型等。	2
C013	習慣	例如：抽煙、喝酒等。	2
C014	個性	例如：個性等之評述意見。	2
家庭情形			
C021	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。	2

附件十五：個人資料類別隱私衝擊分級表（第1版）（本附件未修正）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
C022	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。	2
C023	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。	2
C024	其他社會關係	例如：朋友、同事及其他除家庭之外之關係等。	2
社會情況			
C031	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。	2
C032	財產	例如：所有或具有其他權利之動產或不動產等。	2
C033	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。	2
C034	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。	2
C035	休閒活動及興趣	例如：嗜好、運動及其他興趣等。	2
C036	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。	2
C037	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。	2
C038	職業	例如：學校校長、民意代表或其他各種職業等。	2
C039	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。	2
C040	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。	3
C041	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。	3

附件十五：個人資料類別隱私衝擊分級表（第1版）（本附件未修正）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
教育、考選、技術或其他專業			
C051	學校紀錄	例如：大學、專科或其他學校等。	1
C052	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。	1
C053	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。	2
C054	職業專長	例如：專家、學者、顧問等。	1
C055	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。	2
C056	著作	例如：書籍、文章、報告、視聽出版品及其他著作等。	1
C057	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。	2
C058	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。	2
受僱情形			
C061	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。	2
C062	僱用經過	例如：日期、受僱方式、介紹、僱用期間等。	2
C063	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。	2
C064	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。	2
C065	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。	2
C066	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。	3
C067	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。	2

附件十五：個人資料類別隱私衝擊分級表（第1版）（本附件未修正）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
C068	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。	2
C069	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。	1
C070	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。	1
C071	工作之評估細節	例如：工作表現與潛力之評估等。	2
C072	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。	1
C073	安全細節	例如：密碼、安全號碼與授權等級等。	3
財務細節			
C081	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。	2
C082	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。	2
C083	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。	2
C084	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。	2
C085	外匯交易紀錄		2
C086	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。	2
C087	津貼、福利、贈款		2
C088	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。	2
C089	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。	2

附件十五：個人資料類別隱私衝擊分級表（第1版）（本附件未修正）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
C091	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。	2
C092	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。	2
C093	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。	2
C094	賠償	例如：受請求賠償之細節、數額等。	2
商業資訊			
C101	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。	2
C102	約定或契約	例如：關於交易、商業、法律或其他契約、代理等。	2
C103	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。	1
健康與其他			
C111	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。	3
C112	性生活		3
C113	種族或血統來源	例如：去氧核糖核酸資料等。	3
C114	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。	3
C115	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。	3
C116	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。	3
C117	政治意見	例如：政治上見解、選舉政見等。	2

附件十五：個人資料類別隱私衝擊分級表（第1版）（本附件未修正）

個資類別代碼	個資類別項目	個資類別說明	隱私衝擊等級
C118	政治團體之成員	例如：政黨黨員或擔任之工作等。	2
C119	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。	2
C120	宗教信仰		2
C121	其他信仰		2
其他各類資訊			
C131	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。	1
C132	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。	1
C133	輻射劑量資料	例如：人員或建築之輻射劑量資料等。	2
C134	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。	3

經濟部標準檢驗局（○○分局）

個人資料安全事件通報單

由通報單位/分局之個人資料保護聯絡人員填寫		
單位/分局		
個人資料保護聯絡人員	職稱/姓名	
	聯絡方式	
個人資料保護專責人員	職稱/姓名	
	聯絡方式	
通報時間	年 月 日 時 分	
事件紀錄	發生時間	年 月 日 時 分
	發生地點	
	事件發生單位	<input type="checkbox"/> 單位：_____ <input type="checkbox"/> 委外廠商：_____
	個人資料承辦人	
	事件說明	
	個人資料範圍	
	個人資料儲存媒體	<input type="checkbox"/> 紙本 <input type="checkbox"/> 電子檔案 <input type="checkbox"/> 系統資料庫 <input type="checkbox"/> 光碟片 <input type="checkbox"/> USB 碟 <input type="checkbox"/> 可攜式硬碟 <input type="checkbox"/> 記憶卡 <input type="checkbox"/> 其他：_____
本局個人資料保護推動執行小組（以下簡稱本小組）行政組填寫		
初步分析	本小組行政組受理通報時間	年 月 日 時 分
	儲存媒體所實施之控制與對當事人權益損害分析	

附件十六：個人資料安全事件通報單（第1版）（本附件未修正）

	<p>事件判斷及通報應變</p>	<p> <input type="checkbox"/>非個人資料安全事件（不處理，逕予結案） <input type="checkbox"/>疑似個人資料安全事件（持續觀察，暫不處理） <input type="checkbox"/>依儲存媒體實施之控制強度，判斷應不致於損害當事人權益。 補償性處理：_____ </p> <p> <input type="checkbox"/>屬個人資料安全事故，執行以下行動： </p> <ol style="list-style-type: none"> 電子資料通報應通報資訊服務台 <ul style="list-style-type: none"> <input type="checkbox"/>非屬電子資料 <input type="checkbox"/>電子資料，通報時間 年 月 日 時 分 24小時內組成應變小組（依附件十五「個人資料類別隱私衝擊分級表」進行分級） <ul style="list-style-type: none"> <input type="checkbox"/>第1級或第2級： <ul style="list-style-type: none"> <input type="checkbox"/>由發生個人資料安全事故之單位主管或分局之分局長召集，其在受託廠商發生時，由承辦單位主管或分局之分局長召集。 <input type="checkbox"/>應變小組成員，由發生個人資料安全事故之單位、分局或委外案件承辦單位、分局之個人資料保護專責人員、聯絡人員、個人資料承辦人及應變相關作業人員組成。 <input type="checkbox"/>第3級： <ul style="list-style-type: none"> <input type="checkbox"/>由本小組召集。 <input type="checkbox"/>應變小組成員，由發生個人資料安全事故之單位或分局、委外案件承辦單位或分局之單位主管或分局長、該單位或分局之個人資料保護專責人員、聯絡人員、個人資料承辦人及應變相關作業人員組成。 <p>成立時間 年 月 日 時 分</p> <ol style="list-style-type: none"> 通報各級長官 <ul style="list-style-type: none"> <input type="checkbox"/>資訊安全長 年 月 日 時 分 <input type="checkbox"/>主任秘書 年 月 日 時 分 <input type="checkbox"/>法務室主任 年 月 日 時 分 <input type="checkbox"/>資訊室主任 年 月 日 時 分 外部通報：通報經濟部個人資料保護推動執行小組 通報時間 年 月 日 時 分 通知當事人：（附件十七「通知當事人文稿範例」） <ul style="list-style-type: none"> <input type="checkbox"/>言詞 <input type="checkbox"/>書面 <input type="checkbox"/>電話 <input type="checkbox"/>簡訊 <input type="checkbox"/>電子郵件 <input type="checkbox"/>傳真 <input type="checkbox"/>電子文件 <input type="checkbox"/>其他：_____ <p>通知時間 年 月 日 時 分</p>
核定		
<p>通報單位/分局</p> <p>聯絡人員 專責人員</p>	<p>本小組行政組主辦單位</p>	<p>執行秘書</p> <p>召集人</p>

個人資料電子文書檔案密碼清冊

注意事項：

- 一、含有個人資料之電子文書檔案儲存時，應以加密軟體加密保護。設定密碼之個人資料電子文書檔案，應將密碼及相關資訊記錄於下表，原始檔案及備份檔案位置皆應記錄。
- 二、承辦人設定密碼時，應採用安全強度足夠之密碼，工作變更時列入移交，取得他人移交之加密電子檔案後應變更加密密碼。
- 三、本清冊應以密件文書方式保護，並告知所屬主管密碼清冊之所在。

單位		檔案承辦人		單位主管	
個人資料檔案名稱	儲存位置	產生日期	讀取密碼	可存取人員	備註

個人資料檔案禁止攜出清冊

單位		主管核定		更新日期	
----	--	------	--	------	--

本單位之個人資料檔案採以下攜出管理政策(勾選一政策選項)：

- ☐ 本單位保有之個人資料檔案禁止攜出辦公場所，有特例時每次須簽核後方得攜出。
- ☐ 本單位保有之個人資料檔案以下所列項目為禁止攜出辦公場所之檔案。
- ☐ 本單位保有之個人資料檔案除以下所列項目可攜出外，其餘皆不可攜出，有特例時每次須簽核後方得攜出。

<input type="checkbox"/> 禁止攜出個人資料檔案名稱	
<input type="checkbox"/> 可攜出個人資料檔案名稱	
個人資料檔案名稱 ^註	備註

註：「個人資料檔案名稱」，請依「個人資料檔案彙整表」（附件十二）填具之內容填寫。