財政部關務署臺中關宣導事項

◎關務署於110年10月19日以台財關字第1101027108號令發布修正「報關業設置管理辦法」第18條、第24條、第25條，增訂報關業員工因海關職務有關行為，對於海關執法人員施以不法暴力行為，經海關查明屬實者，專責報關人員不得執業、廢止執業登記並註銷報關證；領有報關證員工，註銷報關證且5年內不得再受僱辦理報關業務。另對該不法員工所屬報關業者，增訂海關得裁處警告或罰鍰、停止6個月以下之報關業務或廢止其報關業務證照。

◎保護智慧財產權

一、進口報關

（一）業者於進口報關時於貨名欄報明商標以備查核。

（二）業者於進口報關前備具商標權或著作權授權證明文件或無侵權情事之證明文件，以備海關查核(當海關查驗關員認有需要時提供海關查核，但無須於報關時事先提供)。

二、出口報關

（一）報運貨物出口時，應於出口報單之商標欄位正確申 報商標，若無商標者亦應於該欄位申報無商標，以免遭海關移送經濟部國際貿易局裁處。

（二）報運預錄式光碟出口時，應於出口報單之貨名欄正 確申報光碟來源識別碼之模具碼，若無來源識別碼者亦應申報無來源識別碼，以免遭海關移送經濟部國際貿易局裁處。

三、當海關發現進出口貨物外觀顯有侵害商標權或著作權之虞時，會即刻通知商標權或著作權人於規定時間內到海關進行侵權認定，並於3(或6)個工作日內提出侵權證明文件，海關亦會同時通知進出口人於3(或6)個工作日內提供授權文件或其他證明無侵權情事文件，請業者於接獲海關通知時配合相關規定時程辦理。

四、商標權及著作權提示保護制度宣導

（一）商標權人及著作權人向海關申請提示保護及申請延長提示保護案件自103年10月1日起提供線上申辦作業，以達電子化服務民眾為導向之目的。

（二）依據「海關執行商標權益保護措施實施辦法」第 4條規定，海關核准之提示保護期間，為自核准之日起至商標權期間屆滿日止。提示保護期間，有關申請人資訊、代理人資訊、提示保護真品及侵權物特徵文字說明、圖像電子檔及其他事項資訊，如有變更，應向關務署申請變更。

（三）線上申辦作業入口網站連結路徑為：

http://portal.sw.nat.gov.tw/ →簡易申辦 →智慧財產權

◎報關業應訂定「報關業個人資料檔案安全維護計畫」，並置放營業場所備查。為免報關業未依本辦法訂定個人資料檔案安全維護計畫而違反個人資料保護法（下稱個資法）第27條第2項規定，致受同法第48條處罰（罰鍰金額新臺幣20萬元以下），爰於關務署外部網頁建立「報關業者個資資訊專區」，供下載旨揭計畫參考範本及個人資料安全維護自我檢查表（網頁下載路徑：關務署/首頁/資訊匯流/機關（公開）資料/個資法公開專區/報關業者個資資訊專區），俾利充分瞭解規範內容及具體執行方式。提供之上開計畫範本僅供參考，報關業者得依實際需要自行調整，但均須遵守個資法及本辦法相關規定。

參考範本

公司名稱

（公司或商業）個人資料檔案安全維護計畫

*範本僅供參考，請依公司或商業內部管理作業程序訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法等相關事項。

壹、業者之組織及規模

一、業者名稱：_____

二、負責人：

三、統一編號：_____

四、事業類別：☐報關業

五、營業地址：

六、員工人數 _____人 (全公司人數 15 報關業人數 5)

（請加蓋公司或商業及負責人章）

蓋公司或商業印鑑章	蓋負責人印鑑章

貳、個人資料檔案之安全維護管理措施（計畫內容）

一、依據：個人資料保護法第二十七條第三項規定及報關業個人資料檔案安全維護管理辦法第二條規定辦理。

二、目的：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本公司（商業）所屬人員應依本計畫辦理個人資料檔案安全管理及維護事宜。

三、管理人員及資源：

(資訊專業 ; 依個別公司狀況)

（一）管理人員：

1、配置人數：＿＿＿＿人。（建議至少配置1名管理人員）

2、職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並向負責人提出報告。

（二）預算：每一年新臺幣＿＿＿＿＿萬元。（包含管理人員薪資、設備費用等，依實際狀況填寫）**(依個別公司規模)**

（三）個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，[illegible]所保有個人資料檔案安全，以防止個人資料

四、個人資料之範圍

（一）特定目的：＿＿＿＿＿＿

（註：本項請依「**個人資料保護法之特定目的及個人資料之類別**」，說明特定目的項目，例如：人事管理(〇〇二)、全民健康保險、勞工保險、國民年金保險或其他社會保險(〇三一)、消費者、客戶管理與服務(〇九〇)等。）

（二）個人資料：本計畫所稱自然人之個人資料，係指客戶姓名、出生年月日、國民身分證統一編號、護照號碼、聯絡方式、信用卡號等，及其他得以直接或間接方式識別該個人之資料。

五、風險評估及管理機制：

（一）風險評估：

1、經由本公司（商業）電腦下載或外部網路入侵而外洩。

2、經由接觸書面契約書類而外洩。

3、員工及第三人竊取、毀損或洩漏。

4、業間互為傳輸時之外洩（包括分公司間傳輸、與相關業者間

〇〇二 人事管理
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
〇九〇 消費者、客戶管理與服務
〇六九 契約、類似契約或其他法律關係事務

傳輸等）。

（二）管理機制：

1、藉由使用者代碼、識別密碼設定及文件妥適保管。

2、定期進行網路資訊安全維護及控管。

3、電磁資料視實際需要以加密方式傳輸。

4、加強對員工之管制及設備之強化管理。

六、個人資料蒐集、處理及利用管理措施：

個資法第 8 條

（一）直接向當事人蒐集個人資料時，應明確告知以下事項：

1、公司（商業）名稱。

2、蒐集目的。

3、個人資料之類別。

4、個人資料利用之期間、地區、對象及方式。

5、當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

6、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。

（二）所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

（三）報關業得為辦理本計畫之特定目的內，進行個人資料蒐集、處理、利用，於委託期限屆滿時應主動刪除或銷毀。但因法令規定、執行業務所必須或經書面同意者，不在此限。

（四）利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。

（五）當事人表示拒絕行銷或請求閱覽、製給複製本、補充或更正

(必須有1位聯絡人;離職時並須更新)

、停止蒐集、處理、利用或刪除其個人資料時，聯絡窗口為：_____電話為：(　)_____，並將聯絡窗口及電話等資料，揭示於本公司（商業）營業處所或網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

（六）負責保管及處理個人資料檔案之員工，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

（七）本公司（商業）員工如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（八）由指定之管理員工定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

（九）本公司（商業）如有委託他人（或他公司或商業）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。（如未委託他人則可選擇加以刪除）

（十）所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

（十一）本公司（商業）因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

七、事故之預防、通報及應變機制：

（一）預防：

1、本公司（商業）員工如因其工作職掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使

用範圍及使用權限內為之。

2、本公司（商業）對內或對外從事個人資料傳輸時，加強管控避免外洩。

3、加強員工教育宣導，並嚴加管制。

（二）通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司（商業）負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2、對於個人資料遭竊取之當事人，應以適當方式通知使其知悉及本公司（商業）個人資料外洩事實、已採取之處理措施、客服電話窗口等資訊。

3、自發現事故時起算七十二小時內，依附表格式以電子郵件方式通報財政部關務署(報關業個資外洩監督通報專用信箱：PDPA@customs.gov.tw)，並應視案情發展適時通報處理情形，以及將整體查處過程、結果與檢討等函報財政部關務署。

4、針對事故發生原因研議改進措施。

八、資料安全管理、員工管理及設備安全管理：

（一）資料安全管理：

1、電腦存取個人資料之管控：

（1）本公司（商業）所屬員工應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。個人資料使用完畢，應即退出電腦使用檔案，不得留置於電腦上。下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於專用抽屜內上鎖保管。

（2）本公司（商業）員工如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（3）個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。

（4）定期進行電腦系統防毒、掃毒之必要措施。

（5）重要個人資料（如護照號碼、國民身分證統一編號）應另加設管控密碼，非經陳報公司（商業）主管核可，並取得密碼者，不得存取。

（6）建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

2、紙本資料之保管：

（1）本公司（商業）保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管有開啟調閱權限，其他所屬人員因業務需要而須調閱或使用個人資料者，應提出申請，經業務主管人員同意後調閱或使用。員工非經公司（商業）負責人或營業處所主管同意不得任意複製或影印。

2）儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及防火設備。

（3）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處

理。

（二）人員管理：

1、本公司（商業）依業務需求，應設定所屬員工（例如主管、非主管員工）不同之權限，以控管其個人資料之情形。

2、本公司（商業）所屬人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。專屬帳號密碼均應保密，不得

3、本公司（商業）員工每_____天（週、月）應變更識別密碼乙次，並於變更識別密碼後始可繼續使用電腦。

4、本公司（商業）員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

5、本公司（商業）與員工所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

6、因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後開放權限利用。

7、本公司（商業）所屬人員均應簽署保密協定，就於任職期間因業務所接觸個人資料均負保密義務。

8、負責個人資料檔案管理人員於職務異動時，應將保管之檔案資料移交，接辦人員應另行設定密碼。

（三）設備安全管理：

1、建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關

安全措施。

2、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

3、應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。

4、本公司（商業）保有之個人資料檔案應定期（例如：每二週）備份。

5、重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。

6、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司（商業）負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除。

7、更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。

九、資料安全稽核機制：

一）本公司（商業）定期（每年至少乙次）辦理個人資料檔案安全維護稽核，查察本公司（商業）是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1、確認不符合事項之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄查察情形及結果。

（二）前項查察情形及結果應載入稽核報告中，由公司（商業）負責人簽名確認。

十、使用記錄、軌跡資料及證據保存：

本公司（商業）建置個人資料之電腦，其個人資料使用查詢紀錄，每年需將該紀錄檔備份並設定密碼，另亦將儲存該紀錄之儲存媒介物保存於適當處所以供備查。

（註：本項請依實際情形說明業者如何保存，例如：個人資料使用查詢紀錄、自動化機器設備之軌跡資料（電腦設備或其他相關之證據資料須加以保存並製作備份保存於適當處所），以供必要時說明其所訂計畫之執行情況。）

十一、保有個人資料達一萬筆者所採行之資訊安全措施（未達者可以自行刪除）：

（一）使用者身分確認及保護機制。

（二）個人資料顯示之隱碼機制。

（三）網際網路傳輸之安全加密機制。

（四）個人資料檔案及資料庫之存取控制與保護監控措施。

（五）防止外部網路入侵對策。

（六）非法（或異常）使用行為之監控與因應機制。

前項所定防止外部網路入侵對策及非法（或異常）使用行為之監控與因應機制等措施，應定期演練（每年至少乙次）及檢討改善。

（註：本項請依實際情形說明所採行之資訊安全措施、定期演練及檢討改善等作業規劃，以供必要時說明執行情況。）

十二、認知宣導及教育訓練：

（一）本公司（商業）員工每年計有___人參與相關單位辦理之個

(個人資料；法人非應列管)

(依公司人數狀況)

人資料保護法基礎教育宣導及數位學習教育訓練至少＿＿＿＿小時，以促使員工知悉應遵守個人資料保護法相關規定。前述教育宣導及訓練並應留存紀錄（例如：簽名冊等文件）

（二）對於新進員工應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

十三、個人資料安全維護之整體持續改善：

（一）本公司（商業）將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

（二）針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十四、業務終止後之個人資料處理方法：

本公司（商業）結束營業後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄至少五年（請勾選或填寫下列事項）：

（一）銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

□書面個人資料已送碎紙機絞碎。

□儲存於電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物之個人資料已格式化刪除資料或以物理方式破壞其功能，如折斷光碟片，擊毀硬碟等。

□其他：（請自行填寫）

以上行為請拍照存證（照片需印日期並揭露地點）或錄影存證（影片需有日期並揭露地點）。

（二）移轉：移轉之原因、對象、方法、時間、地點及受移轉對象

(依公司狀況至少 1 小時 e 等公務員線上課程)

得保有該項個人資料之合法依據。

移轉之原因：

□業務需求

□其他（請自行填寫）：

移轉之對象：

移轉之方法：

□紙本傳遞。

□以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物傳遞。

□其他（請自行填寫）：

移轉之時間（請自行填寫）：中華民國_____年____月_____日

移轉之地點（請自行填寫）：

受移轉對象得保有該項個人資料之合法依據：_____

_____

（三）其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

其他刪除、停止處理或利用之方法（請自行填寫）：

其他刪除、停止處理或利用之時間（請自行填寫）：

其他刪除、停止處理或利用之地點（請自行填寫）：

附表

<table>
<tr><td colspan="4">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td rowspan="5">業者名稱
_____
通報機關
_____</td><td colspan="3">通報時間：　年　月　日　時　分</td></tr>
<tr><td colspan="3">通報人：　　簽名(蓋章)</td></tr>
<tr><td colspan="3">職　稱：</td></tr>
<tr><td colspan="3">電　話：</td></tr>
<tr><td colspan="3">Email ：
地　址：</td></tr>
<tr><td>事件發生時間</td><td colspan="3"></td></tr>
<tr><td rowspan="6">事件發生種類</td><td>□竊取</td><td colspan="2" rowspan="3">個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□洩漏</td></tr>
<tr><td>□竄改</td></tr>
<tr><td>□毀損</td><td colspan="2" rowspan="3">□一般個資_____筆
□特種個資_____筆</td></tr>
<tr><td>□滅失</td></tr>
<tr><td>□其他侵害事故</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="3"></td></tr>
<tr><td>損害狀況</td><td colspan="3"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="3"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="3"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="3"></td></tr>
<tr><td>是否於發現個資外洩後七十二小時內通報</td><td colspan="3">□是　□否，理由：</td></tr>
</table>