附件一

種苗業者應採行適當之個人資料保護安全措施

※法令依據：按個人資料保護法（以下簡稱本法）第27條第1項規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

項目	採　行　措　施
個人資料保護規　　劃	1.配置管理人員及相當資源。 2.界定個人資料之範圍並定期清查。 3.依已界定之個人資料範圍及個人資料蒐集、處理、利用之流程，分析可能產生之風險，並根據風險分析之結果，訂定適當之管控措施。 4.就所保有之個人資料被竊取、竄改、毀損、滅失或洩露等事故，採取適當之應變措施，以控制事故對當事人之損害，並通報有關單位及以適當方式通知當事人；於事後研議預防機制，避免類似事故再度發生。 5.對於所屬人員施以宣導或教育訓練。
個人資料管理程序	1.檢視蒐集、處理個人資料之特定目的，及是否符合免告知之事由，以符合本法第8條及第9條關於告知義務之規定。 2.檢視蒐集、處理個人資料是否符合本法第19條規定，具有特定目的及法定要件，及利用個人資料是否符合本法第20條第1項規定於特定目的內利用；於特定目的外利用個人資料時，檢視是否具備法定特定目的外利用要件。 3.委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第8條規定為適當之監督，並明確約定相關監督事項與方法。 4.當事人行使本法第3條所規定之權利時，確認是否為個人資料之本人，並遵守本法第13條有關處理期限之規定。 5.為維護所保有個人資料之正確性，檢視於蒐集、處理或利用過程，是否正確，發現個人資料不正確時，適時更正、補充或通知曾提供利用之對象；個人資料正確性有爭議者，依本法第11條第2項規定處理之方式。 6.檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；確認特定目的消失或期限屆滿時，依本法第11條第3項規定處理。
訂定個人資料檔案安全維護計畫	1.資料安全管理措施： (1)運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒介物之規範。 (2)針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

項目	採 行 措 施
	(3)作業過程有備份個人資料之需要時，比照原件，依本法規定予以保護之。 (4)個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該媒介物洩漏個人資料。 (5)委託他人執行前款行為時，對受託人依本法施行細則第8條規定為適當之監督，並明確約定相關監督事項與方式。 2.人員管理措施： (1)依據作業之需要，適度設定所屬人員不同之權限並控管其接觸個人資料之情形。 (2)檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。 (3)與所屬人員約定保密義務。 3.設備安全管理措施： (1)保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，依據作業內容之不同，實施適宜之進出管制方式。 (2)所屬人員妥善保管個人資料之儲存媒介物。 (3)針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。 4.業務終止後個人資料處理措施： (1)銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 (2)移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 (3)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。 5.請種苗業者訂定個人資料檔案安全維護計畫(得參照範例訂定)，報由直轄市、縣市政府核備後實施。
檢視、修訂及紀錄個人資料保護事宜	1.種苗業者應參酌執行業務現況、技術發展及法令變化等因素，檢視或修訂個人資料保護事項。 2.種苗業者應就個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據建立保存機制，以供說明執行個人資料保護事項之情況。

附件二

○○公司（場、園）個人資料檔案安全維護計畫範本

蓋總公司印鑑章

壹、組織及規模

一、 代表人（負責人）：○○○

二、 公司地址：○○市○○區○○路（街）○段○號

三、 員工人數： ○○人

蓋代表人印鑑章

貳、個人資料檔案之安全維護管理措施(計畫內容)

一、管理人員及資源

（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。

（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，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

二、個人資料之範圍

（一）特定目的及類別：

1.特定目的：

○○二　人事管理

一三八　農產品交易

一三九　農產品推廣資訊

2.類別：

C一○一　資料主體之商業活動

C一○二　約定或契約

C一○三　與營業有關之執照

（請依公告之「個人資料保護法之特定目的及個人資料之類別」調整）

（二）個人資料：本計畫所稱自然人之個人資料，除係指姓名、出生年月日、國民身分證統一編號、聯絡方式及其他得以直接或間接方

式識別該個人之資料。(依實際蒐集之個人資料調整。)

三、風險評估及管理機制

(一)風險評估

1、經由本公司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、組織或個人間互為傳輸時之外洩(包括分公司間傳輸、同業間傳輸)。

(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。

四、個人資料蒐集、處理及利用管理措施

(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)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、停止蒐集、處理、利用或刪除其個人資料時，連絡窗口為：○○○ ；電話為：○○○○○○。並將聯絡窗口及電話等資料，揭示於本公司營業處所或公司網頁。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）本公司如有委託他人（或他公司）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。

（如未委託他人則可以選擇加以刪除）

（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。

五、事故之預防、通報及應變機制

（一）預防：

1、本公司員工如因其工作執掌而須輸出、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、滅失或洩漏即向交通部觀光局及公司負責人通報，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旅客，應以適當方式通知使其知悉及本公司個人資料外洩事實、已採取之處理措施、客服電話窗口等資訊。

3、針對事故發生原因研議改進措施。

六、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）個人資料檔案儲存在電腦硬式磁碟機上者，應在電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）本公司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。

（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（如國民身分證統一編號）應另加設管控密碼，非經陳報公司主管核可，並取得密碼者，不得存取。

（6）本公司所屬人員禁止使用私人可攜式設備（例如 USB 隨身碟、外接硬碟、筆記型電腦、手機、記憶卡等）儲存本公司所保有個人資料檔案。

2、紙本資料之保管：

（1）對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，員工非經公司負責人或營業處所主管同意不得任意複製或影印。

（2）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。

3、電子資料之保管：

（1）本公司(市場)所保有個人資料檔案應以加密方式儲存，僅經授權之所屬人員得開啟處理、利用。

（2）以網際網路傳輸個人資料時，亦應以加密方式為之。

（二）員工管理

1、本公司依業務需求,得適度設定所屬員工(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、本公司員工每◯天（週、月）應變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。（建議180天）

3、本公司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。

4、本公司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)。

（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、公司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、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。

七、資料安全稽核機制

（一）本公司定期(每年至少1次)辦理個人資料檔案安全維護稽核，查察本公司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，由公司負責人簽名確認。

八、使用記錄、軌跡資料及證據保存

本公司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公司如何保存，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。）

九、認知宣導及教育訓練

（一）本公司每年員工〇人參與個人資料保護法基礎教育宣導或數位學習教育訓練至少◯小時，使員工知悉應遵守之規定。前述教育宣導及訓練應留存紀錄（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、個人資料安全維護之整體持續改善

（一）本公司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。

十一、業務終止後之個人資料處理方法

本公司結束營業後，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 000 年 00 月 00 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：依據個人資料保護法第 00 條規定…。

（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）：