

○○ (股份)有限公司個人資料檔案安全維護計畫(範本)

壹、組織及規模

- 一、名稱：
- 二、旅宿專用標識編號：
- 三、代表人：
- 四、公司地址：

蓋總公司印鑑章

蓋代表人
印鑑章

貳、個人資料檔案之安全管理措施(計畫內容)

一、配置管理之人員及相當資源

(一)管理人員：

- 1、配置人數：○人。(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，並向代表人提出報告。

(二)預算：每年新臺幣○萬元。(依實際狀況填寫)

(三)本公司遵循個人資料保護法令關於蒐集、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、界定蒐集、處理及利用個人資料之範圍

(一)特定目的：管理業務、契約、類似契約或其他法律關係事務、消費者、客戶管理與服務等運用、人事管理等運用(類別：識別類、社會情況類)。

(二)個人資料：指自然人(包含旅客、消費者、從業人員、導遊及領隊等)之姓名、出生年月日、國民身分證統一編號、護照號碼、信用卡卡號、聯絡方式及其他得以直接或間接方式識別該個人之資料。

三、個人資料之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、旅宿業間互為傳輸時之外洩(包括分公司間傳輸)。

(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、電子資料檔案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、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。

(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，將危及正常營運或大量當事人權益，應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，並於知悉事故 72 小時內依附表通報交通部觀光署。

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、預防之措施。

五、個人資料蒐集、處理及利用之內部管理程序

(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告知事項。

(三)本公司為辦理本計畫之特定目的，得進行個人資料蒐集、處理、利用，於特定目的消失或委託期限屆滿時應主動刪除或銷毀。但因法令(如旅館業管理規則、民宿管理辦法等)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，聯絡窗口：○○○(需為執行業

務人員)；電話：○○○○○○○，並將聯絡資訊揭示於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，其職務有異動或離職時，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)本公司如委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督並與其明確約定相關監督事項。
- (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。

六、設備安全管理、資料安全管理及人員管理措施

(一)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、本公司之個人資料檔案應定期備份(如：每二週)。
- 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，本公司代表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。

(二)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，非經陳報公司主管核可，並取得密碼者，不得存取。

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，員工非經公司代表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。

(三)人員管理

- 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，並定期檢視權限之適當性及必要性。
- 2、本公司員工每○天/週/月(需低於90日、12週或3個月)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。
- 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；簽訂勞務契約亦列入保密條款及相關之違約罰則，以確保執行業務期間對於個人資料內容之保密義務。
- 4、員工或為旅宿業執行業務者與公司終止契約時，將立即取消其使用者代碼(帳號)及識別密碼，其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書。

七、認知宣導及教育訓練

- (一)本公司每年應定期或不定期對員工施以基礎個人資料保護認知宣導及教育訓練至少2小時，使員工明瞭個人資料保護相關法令、責任範圍及個人資料保護事項之機制、程序及措施；對於新進員工應給予特別指導，以利遵循相關規定。
- (二)前述教育宣導及訓練應留存紀錄(例如：簽名冊等文件)。

八、個人資料安全維護稽核機制

- (一)本公司每年至少辦理1次個人資料安全維護稽核，檢查是否落實本計畫規範事項，針對檢查結果不合法令及潛在不符合之風險，應即改善，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、紀錄檢查情形及結果。

(二)前項檢查結果應載入稽核報告中，由公司代表人簽名確認，並留存相關紀錄至少5年。

九、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、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、個人資料安全維護之整體持續改善

(一)本公司將隨時參酌業務及依據計畫執行狀況，注意相關社會輿情、技術發展及法規增修等因素，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合法令之虞者，應即規劃改善。

十一、業務終止後之個人資料處理方法

本公司業務終止後，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5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；儲存於電腦磁碟及其他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： (股份)有限公司

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)：

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○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、時間或地點請自行填寫)：

中華民國○○○年○○月○○日訂定

附表

個人資料侵害事故通報與紀錄表

通報時間： 年 月 日 時 分

名稱：	(股份)有限公司		
通報人：			
職稱：			
電話：			
Email：			
地址：			
事件發生時間	年	月	日 時 分
事件發生種類	<input type="checkbox"/> 竊取 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 其他侵害 事故		
個資侵害之總筆數(大約)	<input type="checkbox"/> 一般個資	筆	
	<input type="checkbox"/> 特種個資	筆	
發生原因及事件摘要			
損害狀況			
個資外洩可能結果			
擬採取之因應措施			
擬採通知當事人之時間及方式			
是否於發現個資外洩後 72 小時通報主管機關	<input type="checkbox"/> 是 <input type="checkbox"/> 否，理由		

註 1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註 2：上開 72 小時通報主管機關，例假日均納入時效計算。