附件1

觀光產業個人資料檔案安全稽核檢查表

公司名稱： □有限公司 □股份有限公司								
經營業別：旅行業/觀光遊樂業/觀光旅館業/旅館業/民宿(請自行圈選)								
市招: 登記證編號:								
營業地址:								
查核日期： 年 月 日					相關法規			
查核項目	查核內容	查核結果	說明	備註	個人資料保護法	個人資料保護法施行細則	交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法	臺南市政府對非公務機關實施個人資料保護行政檢查及聯繫作業要點（第5點-實施檢查項目）
1.消費者個人資料檔案安全維護計畫	訂定「消費者個人資料檔案安全維護計畫」	□符合 □不符合 □不適用		按交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條訂定安全維護計畫。	§27 §48Ⅱ、Ⅲ	§12	§1、4、5、6	
2.配置管理之人員及相當資源	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。	§27Ⅰ、3~10、11、12、13、14、19~21、22~27	§12	§5~12、13~22	
3.界定個人資料之範圍	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。	§27Ⅰ	§12	§6、7	
4.個人資料之風險評估及管理機制	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。	§27Ⅰ、Ⅱ	§12	§6Ⅲ、7、8	（三）遵守中央目的事業主管機關依個資法第二十一條規定限制國際傳輸之命令或處分情形。 （十）防止個人資料被竊取、竄改、毀損、滅失或洩漏之安全措施辦理情形。 （十一）個人資料檔案安全維護計畫或業務終止後個人資料處理方法之訂定情形。
5.事故之預防、通報及應變機制	5.1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。	§27Ⅰ	§12	§9	
	5.2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	□符合 □不符合 □不適用		請說明應變機制對通知當事人之作法。	§12、27	§12、22	§9	（七）違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害事件，後續查明及通知當事人之情形。

	形，及後續供當事人查詢之專線與其他查詢管道？							
	5.3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。	§27 I	§12	§9	
	5.4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。	§27 I	§12	§9	
6.蒐集、處理、利用作業	6.1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。	§19、20		§10	（一）蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料情形。 （二）蒐集、處理或利用前款以外其他個人資料之情形。
	6.2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。	§19、20		§10	（一）蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料情形。 （二）蒐集、處理或利用前款以外其他個人資料之情形。
	6.3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。	§19、20		§10	（一）蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料情形。 （二）蒐集、處理或利用前款以外其他個人資料之情形。
	6.4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		請說明蒐集個資並取得當事人同意之情形。	§19、20		§10	（一）蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料情形。 （二）蒐集、處理或利用前款以外其他個人資料之情形。
	6.5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。	§2、7、8、9	§16	§10、11	（四）遵守蒐集個人資料之告知義務情形。 （五）依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本與依法定期間

								准駁及通知請求人之情形。 （六）維護個人資料正確性之情形。
	6.6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。	§8、9、20	§16	§10、11、13	（八）利用個人資料行銷者，當事人表示拒絕接受行銷時，停止利用其個人資料行銷之情形。 （九）於首次行銷時，提供當事人表示拒絕接受行銷之方式，並支付所需費用之情形。
	6.7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。	§8、9、20	§16	§10、11、13	（八）利用個人資料行銷者，當事人表示拒絕接受行銷時，停止利用其個人資料行銷之情形。 （九）於首次行銷時，提供當事人表示拒絕接受行銷之方式，並支付所需費用之情形。
7. 資料安全管理及人員管理	7.1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。	§11、13			
	7.2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。	§27 I	§12	§15	
	7.3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。	§27 I	§12	§15	
	7.4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。	§27 I	§12	§15	
	7.5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。	§27 I	§12	**§14**	
	7.6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。	§27 I	§12	§14	

	7.7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。	§27 I	§12	§14	
8.認知宣導及教育訓練	8.1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。	§27 I	§12	§17	
9. 設備安全管理措施	9.1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。	§27 I	§12	§14	
	9.2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。	§27 I	§12	§14	
	9.3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。	§27 I	§12	§14	
10. 資料安全稽核機制	10.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？	□符合 □不符合 □不適用		請說明稽核之頻率及執行方式，並檢附最近一次之評估報告。	§27 I	§12	§6、7、**18**	
	10.2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。	§27 I	§12	§6、7、8、**18**	
11. 使用紀錄、軌跡資料及證據保存	11.1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？	§11、§27 I	§12	§19	
	11.2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。	§11、§27 I	§12	§19	
	11.3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。	§11、§27 I	§12	§19	
	11.4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。	§11、§27 I	§12	§19	
	11.5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、§27 I	§12	§19	
12. 個人資料安全維護之整體持續改善	12.1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。	§27 I	§12	§6、8	
	12.2是否訂定個人資料管理(或安全維護)辦法並定期檢視更新？	□符合 □不符合 □不適用		請檢附個人資料管理(或安全維護)辦法以及完整之版本資訊，包含但不限於日期、提報人及核定人等相關資訊。	§27 I	§12	§6、8	

13.委託作業	13.1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。	§4	§8	§21	
	13.2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。	§4	§8	§21	
	13.3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。	§4	§8	§21	
	13.4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。	§4	§8	§21	
	13.5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。	§4	§8	§21	
14. 使用資通訊系統蒐集、處理或利用個人資料-消費者個人資料達8千筆，且具對外<u>電子商務服務系統者</u> (交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第16條第3項: 電子商務，係指透過網際網路進行有關商品或服務之廣告、行銷、供應、訂購或遞送等各項商業交易活動。)	14.1是否採行使用者身分確認及保護機制？(基準日：○年○月○日，下同)	□符合 □不符合 □不適用		建議依「交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法」第16條所列項目稽核。 舉例:14.3-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。	§27 I	§12	§16	
	14.2是否採行個人資料顯示之隱碼機制？	□符合 □不符合 □不適用			§27 I	§12	§16	
	14.3是否採行網際網路傳輸之安全加密機制？	□符合 □不符合 □不適用			§27 I	§12	§16	
	14.4是否採行個人資料檔案及資料庫之存取控制與保護監控措施？	□符合 □不符合 □不適用			§27 I	§12	§16	
	14.5是否採行防止外部網路入侵對策？	□符合 □不符合 □不適用			§27 I	§12	§16	
	14.6是否採行非法或異常使用行為之監控與因應機制？	□符合 □不符合 □不適用			§27 I	§12	§9、16	
	14.7前2項之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，是否定期演練及檢討改善？	□符合 □不符合 □不適用			§27 I	§12	§16	
15. 個資存放雲端之安全控管	15.1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)。	§27 I	§12	§16	

16. 發生個資事件之處理	16.1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。	§27 I	§12	§9	
	16.2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。	§27 I	§12	§9	
	16.3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。	§12、27	§12、22	§9	（七）違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害事件，後續查明及通知當事人之情形。
	16.4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。	§27 I	§12	§9	
17. 個人資料庫之共享使用	17.1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。	§2、7、8、9	§16	§10、11	（四）遵守蒐集個人資料之告知義務情形。
	17.2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。	§2、7、8、9	§16	§10、11	（四）遵守蒐集個人資料之告知義務情形。
18. 其他								

檢查結果及後續處理:

受檢業者簽章： （受檢查人或受訪人拒絕簽名者，應附記其事由。由本府工作人員二人簽名證明。）

檢查單位及人員簽名：

檢查機關:臺南市政府觀光旅遊局

協助機關/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。