易飛網國際旅行社（股份）有限公司
個人資料檔案安全維護計畫

壹、旅行業之組織及規模

一、 組織型態：股份有限公司

二、 代表人（負責人）：周育蔚

三、 資本額：新臺幣 302,597,600 元整

四、 公司編號：70464468

五、 公司類別：綜合

六、 公司地址：臺北市中正區光復里衡陽路 51 號 2 樓之 1

七、 員工人數： 221 人

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：

為推動與落實個人資料保護與管理事宜，本公司應設置個人資料保護管理執行小組(以下稱執行小組):

1、 配置人數：20 人。

2、 任務

(1) 個人資料保護政策之擬議。

(2) 個人資料管理制度之推展。

(3) 個人資料風險之評估及管理。

(4) 人員之個人資料保護意識提升及教育訓練之擬議。

(5) 個人資料管理制度基礎設施之評估。

(6) 個人資料管理制度適法性與合宜性之檢視、審議及評估。

(7) 其他個人資料保護、管理之規劃及執行事項。

3、 組織

本公司設立「個人資料保護管理執行小組」負責推動個資保護管理事宜，其管理組織架構(附圖)如下:

(1) 總召集人:由總經理或其指派之人員擔任之。

(2) 副召集人:由總經理指派之人員擔任之。

(3) 常設委員:由管理部主管、財務會計部主管、銷售部主管或其指派人員擔任之。

(4) 部門個資代表:依個資相關議題，由常設委員召集相關部門主管或其指派之人員擔任之。

4、 職掌

(1) 總召集人:負責核准本公司個資保護管理政策及相關個資管理程序與辦法、執行小組之統籌決策與監督執行業務推行與資源整合運用、啟動緊急應變小組、裁示事件處置方案、調度及安排應對人員、處置狀況進度追蹤。

(2) 副召集人:負責協助總召集人執行工作內容。

(3) 常設委員:負責個人資料保護政策、制度暨相關文件之制定等有關於個人資料保護與管理事宜之規劃、推動與落實。

(4) 部門個資代表:協助推動與落實個人資料保護與管理事宜，並督促各部門人員遵守本辦法之運作與效果之維持，以及個資安全維護及保管事項。

5、 會議之召開及其效力

執行小組應每年至少召開一次會議、或於有必要時、法令變動時、第二級個資事故發生時，由總召集人召集會議，並做成會議記錄，呈總經理核決後，始有效力。

(二)預算：每一年新台幣壹佰萬元。

(三)個人資料保護管理政策：

1、 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。

2、 依據管理政策應制定「個人資料暨隱私權保護政策」，送董事長核定後，公告予本公司所屬人員知悉。

3、 前項政策應敘明本公司所蒐集、處理、及利用個人資料之依據、特定目的及其他相關保護事項。

4、 前項政策之公告以電子郵件、網際網路、或其他足以本公司所屬人員知悉之方式為之。

二、 個人資料之範圍

(一)特定目的：旅行業服務、接受旅客委託代辦入、出國境及簽證手續、履行旅遊契約或類似契約或其他法律關係事務、消

費者旅客管理與服務、辦理責任保險、人事管理、承攬執行接待或引導旅客觀光旅遊業務而收取報酬之導遊、領隊。（類別：識別類、社會情況類）

(二)個人資料：指自然人(含旅客)之姓名、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、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料，以下簡稱「個資」。

(三)個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

(四)蒐集：指以任何方式取得個人資料。

(五)處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

(六)利用：指將蒐集之個人資料為處理以外之使用。

(七)國際傳輸：指將個人資料作跨國（境）之處理或利用。

(八)公務機關：指依法行使公權力之中央或地方機關或行政法人。

(九)非公務機關：指前款以外之自然人、法人或其他團體。

(十)當事人：指個人資料之本人。

三、 風險評估及管理機制

(一)風險評估

1、 管理部每年應至少辦理一次個人資料風險評估與管理作業，依已界定之個人資料範圍及個人資料蒐集、處理與利用之流程，分析可能產生之風險，並根據風險分析之結果，訂定適當的風險管理措施。

2、 凡業務或日常作業涉及個人資料蒐集、處理與利用之部門應參與個人資料風險評估與管理作業，並建立個人資料風險評估清冊。

3、 於業務變動、法令修訂或有必要時，管理部得適時辦理個人資料風險評估與管理作業，相關部門應參與個人資料風險評估與管理作業，並建立或調整個人資料風險評估清冊。

4、 管理部應於相關部門完成風險評估後，召開風險評估與管理會議，審查前項之個人資料風險評估結果並研擬風險處置計畫；風險評估與管理會議之成員為常設委員，於有必要時，得要求相關部門參加會議並協助審查與研擬風險處置計畫。前項個人資料風險處置計畫經總經理簽核後，各部門應依計畫所訂時程，採取相關措施。

5、 個人資料風險評估清冊及風險處置計畫應於參與個人資料風險評估與管理作業相關部門主管簽名確認及總經理核定後，送管理部保存；於有調整時，亦同。

6、 會議之召開及其效力

為落實成效追蹤，各部門應將個人資料風險評估清冊及風險處置計畫執行狀況及追蹤情形於定期會議呈報總經理。

7、 委託他人蒐集、處理與利用個人資料程序(包括分公司間傳輸、同業旅行社間傳輸或其他委外傳輸作業)之風險評估條款，於其後肆、個人資料蒐集、處理及利用管理措施中第(十四)點，詳加規範。

(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。

5、 上述四款於其後第陸條、資料安全管理、員工管理及設備安全管理，詳加規範。

四、 個人資料蒐集、處理及利用管理措施

(一)個人資料蒐集、處理與利用之原則

各部門於蒐集、處理或利用個人資料時，應尊重當事人之權益，依誠實及信用方法為之，遵守個人資料保護法等相關規定，不得於逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

(二)於業務新增時，個人資料蒐集之核定

各部門新增之業務如有涉及個人資料蒐集、處理與利用之

情況,應以簽呈向管理部通報個人資料蒐集之特定目的與特定依據,以及是否必須依個人資料保護法第 8 條或第 9 條規定向當事人告知,並報請總經理核定後,方得進行個人資料之蒐集、處理與利用。

(三)個人資料之蒐集、處理

1、 各部門於蒐集或處理個人資料前,應檢視是否具有特定目的與個人資料保護法第 19 條所定之法定要件之一,包括:

(1) 法律明文規定。

(2) 與當事人有契約或類似契約之關係。

(3) 當事人自行公開或其他已合法公開之個人資料。

(4) 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蒐集者依其揭露方式無從識別特定之當事人。

(5) 經當事人書面同意。

(6) 與公共利益有關。

(7) 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用,顯有更值得保護之重大利益者,不在此限。

(四)告知之方式、告知事項之內容及事項

1、 各部門依個人資料保護法第 8 條或第 9 條之規定,向當事人進行告知時,得依據資料蒐集之情況,採取適當之告知方式,包括:以書面、網頁、電子郵件或其他足使當事人知悉之方式為之。

2、 如係直接向當事人蒐集其個人資料(直接蒐集)時,各部門應於蒐集時,明確告知當事人下列事項:

(1) 機關或單位名稱,即本公司名稱。

(2) 蒐集之目的。

(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) 當事人依個人資料保護法規定得行使之權利及方式如下,並不得預先拋棄或以特約限制之:

A. 查詢或請求閱覽。

B. 請求製給複製本。
C. 請求補充或更正。
D. 請求停止蒐集、處理或利用。
E. 請求刪除。
F. 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。

3、如蒐集非由當事人提供個人資料(間接蒐集)時，各部門應於處理或利用前，明確告知當事人下列事項:

(1)機關或單位名稱，即本公司名稱。
(2)蒐集之目的。
(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)當事人依個人資料保護法規定得行使之權利及方式如下，並不得預先拋棄或以特約限制之：
A. 個人資料來源
B. 查詢或請求閱覽。
C. 請求製給複製本。
D. 請求補充或更正。
E. 請求停止蒐集、處理或利用。
F. 請求刪除。

(五)免告知之事由

1、如係直接向當事人蒐集其個人資料(直接蒐集)時，其免告知事由如下：

(1)依法律規定得免告知。
(2)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
(3)告知將妨害公務機關執行法定職務。
(4)告知將妨害第三人之重大利益。
(5)當事人明知應告知之內容。

2、如蒐集非由當事人提供之個人資料(間接蒐集)時，其免告知事由如下：

(1)有前條第 2 項所列各款情形之一。
(2)當事人自行公開或其他已合法公開之個人資料。

(3) 不能向當事人或其法定代理人為告知。

(4) 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

(5) 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

(6) 上述之告知，得於首次對當事人為利用時併同為之。

(六)使用記錄、軌跡資料與證據保存

1、 本公司應建立個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存，以證明落實本辦法之規定。 前項紀錄、資料或證據之保存期限，除法令另有規定外，應至少保存五年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

2、 保存期限屆滿時，如有延長保存之必要，應以簽呈敘明理由，經總經理核准後，始得延長保存。

(七)個人資料之停止搜集、處理或利用

於有下列情形之一時,除法令另有規定或經當事人書面同意，各部門應刪除或銷毀個人資料，包括：

1、 各部門依特定目的與依據所蒐集之個人資料,除法令另有規定或經當事人書面同意外,應於特定目的消失或保存期限屆滿後，進行刪除與銷毀。

2、 違反個人資料保護法規定蒐集、處理或利用個人資料時。

3、 經當事人請求停止蒐集、處理或利用時。

(八)個人資料的刪除及銷毀

1、 於有下列情形之一時,除法令另有規定或經當事人書面同意，各部門應刪除或銷毀個人資料，包括：

(1) 各部門依特定目的與依據所蒐集之個人資料，除法令另有規定或經當事人書面同意外，應於特定目的消失或保存期限屆滿後，進行刪除與銷毀。

(2) 違反個人資料保護法規定蒐集、處理或利用個人資料時。

(3) 經當事人請求停止蒐集、處理或利用時。

2、 管理部應定期清查其個人資料之刪除與銷毀如需整批進行，應填寫「資料/文件銷毀單」，經權責主管簽核後送管理部，由管理部指派人員一名參與並監督銷毀過程，刪除與銷毀過程結束後應將「資料/文件銷毀單」繳至管理部備查。

3、 但因法令規定（旅行業管理規則第25條第3項：「旅行業辦理旅遊業務，應製作旅客交付文件與繳費收據，分由雙方收執，並連同與旅客簽定之旅遊契約書，設置專櫃保管一年，備供查核。」）、執行業務所必須或經書面同意者，不在此限。

4、 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，並刪除職人員之各項電腦權限，以利管理。

5、 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。

(九)當事人得行使之權利

1、 當事人就其個人資料依個資法規定行使之下列權利，各部門不得要求當事人預先拋棄或以特約限制之：

(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、處理或利用。

(5) 請求刪除。

2、 受理當事人權利行使之方式

當事人得以電話、E-mail、傳真等方式向本公司請求其個資法所定之權利。連絡信箱為wsm@ezfly.com；電話為(02)7725-0800#1681，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。

3、 當事人身分之確認

各部門於收到當事人請求其個資法上之權利時，得請

對方提出相關證件或請當事人以口頭說出其部分個人資料以供本公司核對並確認是否為本人。

4、 依當事人之請求之例外

(1) 於下列情形之一者,各部門得不答覆當事人查詢、提供閱覽或製給複製本之請求，包括：

A. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

B. 妨害公務機關執行法定職務。

C. 妨害該蒐集機關或第三人之重大利益

(2) 於下列情形之一者，各部門得拒絕當事人刪除或銷毀個人資料之請求，包括：

A. 有法令規定或契約約定之保存期限。

B. 有理由足認刪除將侵害當事人值得保護之利益。

C. 其他不能刪除之正當事由。

(3) 如具有拒絕當事人行使權利之事由，各部門應附理由通知當事人。

5、 受理當事人權利行使及申訴之回覆期限及相關規定

本公司受理當事人權利行使回覆期限及相關規定，如下:

(1) 當事人之查詢、閱覽及副本給予請求權

A. 本公司受理當事人查詢、閱覽及副本給予請求時，應填寫「個人資料通報單」，並應於十五日內,為准駁之決定並附理由通知當事人；必要時， 得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

B. 查詢或請求閱覽個人資料或製給複製本者，本公司得酌收必要成本費用。

(2) 當事人之更正、補充、刪除請求權

本公司受理當事人之更正、補充、刪除之請求時，除會員資料之E-mail地址更新外，應填寫「個人資料通報單」並應於三十日內，為准駁之決定並附理由通知當事人；必要時，得予延長，延長之

期間不得逾三十日，並應將其原因以書面通知請求人。

(3) 當事人請求停止蒐集、處理或利用

本公司受理當事人請求停止蒐集、處理或利用其個人資料時，應填寫「個人資料通報單」，除停止行銷目的外，權責單位應於十五日內依請求人提出之原因評估其影響並進行處理，並將處理結果以書面通知請求人。

(十)定期清查

1、 管理部每年應至少一次或不定期辦理個人資料檔案盤點作業，以確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理或利用之個人資料之類別或範圍。

2、 凡業務或日常作業涉及個人資料蒐集、處理與利用之部門應參與個人資料檔案盤點作業，並建立個人資料檔案盤點清冊。

3、 於個人資料檔案盤點時，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、保存期限屆滿而無保存必要者，應依本辦法所定程序，刪除、銷毀或停止處理或利用該個人資料。

4、 於業務變動、法令修訂或有必要時，管理部得適時辦理個人資料檔案盤點作業，相關部門應參與個人資料檔案盤點作業，並建立或調整個人資料檔案盤點清冊。

5、 個人資料檔案盤點清冊應於參與個人資料檔案盤點作業相關部門主管簽名確認及總經理核定後，送管理部保存；於有調整時，亦同。

(十一) 委託他人蒐集、處理與利用個人資料程序

各部門之作業如有委託他人處理時(以下稱委外作業)，若有涉及大量或長期之個人資料蒐集、處理或利用，依下列程序辦理：

1、 委外作業個人資料保護能力之評估

各部門應於受託者接觸本公司個人資料或開始進行個人資料蒐集前，確認該受託者已採取適當安全之必

要措施以保護所蒐集之個人資料，或取得其已實施適當安全維護措施之證明。

2、委外作業書面契約

(1) 委外作業若有必要時本公司應與受託者簽訂書面契約。受託者及其受僱人僅得於本公司指示之範圍、類別、特定目的及期間內，蒐集、處理或利用個人資料。

(2) 於委外合約中應載明要求受託者應依據個資法施行細則第 12 條第 2 項進行適當之安全維護措施，以及下列項目：

A. 本公司對於受託者之適當安全維護措施之具體要求或條件措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

a. 配置管理之人員及相當資源。

b. 界定個人資料之範圍。

c. 個人資料之風險評估及管理機制。

d. 事故之預防、通報及應變機制。

e. 個人資料蒐集、處理及利用之內部管理程序。

f. 資料安全管理及人員管理。

g. 認知宣導及教育訓練。

h. 設備安全管理。

i. 資料安全稽核機制。

j. 使用紀錄、軌跡資料及證據保存。

k. 個人資料安全維護之整體持續改善。

B. 本公司並得要求受託者提供適當安全維護措施定期檢核的頻率、方式及證據。

C. 如受託者無法通過本公司的適當安全維護檢核，本公司有權解除委外合約，受託者並應賠償本公司因此產生之損失。

D. 如需要，本公司得進行受託者之現場稽核，以確保受託者已進行適當安全維護措施，受託者並應支付本公司進行稽核所需之費用。

E. 於合約載明本委託案件不得部份分包或轉包，如需分包或轉包，需取得本公司之事前書面同意。如有複委託情形，應要求受複委託者，執行同於本公司要求受託者之所有條件，並要求受委託廠商協助本公司對於該複委託對象衍生所需之監督義務，並支付其衍生之費用。

F. 確認受託者或其受僱人違反個人資料保護法、其他個人資料保護法律，或其法規命令時，應以書面向本公司通知之事項及採行之補救措施。

G. 本公司如對受託者有保留指示者，委外作業承辦人員應於委外合約中要求監督保留指示之事項。

H. 委託關係終止或解除時，受託者應立即刪除、銷毀為合約目的所蒐集之個資，並出具刪除、銷毀之書面證明或聲明。如受託者之員工、代理人或轉包商因違反合約規定致本公司受有損害時，受託者應負擔損害賠償責任。

(3) 委外業務各部門承辦人員應依採購及付款辦法定期進行供應商評鑑，以監督及確認受託者執行之狀況，並將確認結果記錄於供應商評鑑表。

(十二) 個人資料之利用

1、 各部門於利用個人資料前，應確認是否符合蒐集個人資料之特定目的。

2、 各部門對於個人資料之利用如與原蒐集個人資料之特定目的不相同時，應檢視是否具有個人資料保護法第 20 條所定之法定要件之一，包括：

(1) 法律明文規定。

(2) 為增進公共利益。

(3) 為免除當事人之生命、身體、自由或財產上之危險。

(4) 為防止他人權益之重大危害。

(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蒐集者依其揭露方式無從識別特定之當事人。

(6) 經當事人書面同意。

3、 各部門對於個人資料之利用如與原蒐集個人資料之特定目的不相同時，應向管理部呈報後，經總經理同意後，方得為之。

4、 利用個人資料為行銷之規定

(1) 行銷部門於利用個人資料為行銷時，應確認是否為本公司首次利用個人資料為行銷；如係為首次利用個人資料為行銷，應提供當事人免費表示拒絕接受行銷之方式，包括：電話、電子郵件或其他方式。

(2) 各部門於接獲當事人拒絕行銷之訊息後，應立即停止利用其個人資料為行銷，於系統進行註記，並填寫個資通報單，週知其他部門。

(十三) 個人資料之國際傳輸

1、 管理部應適時注意中央目的事業主管機關是否有限制將個人資料為國際傳輸之規定，並週知各部門。

2、 各部門進行個人資料國際傳輸前，應檢視中央目的事業主管機關是否有限制將個人資料為國際傳輸之規定，並應遵循之。

3、 各部門進行個人資料國際傳輸時，應採取適當的安全措施。

(十四) 個人資料正確性之維持

1、 各部門於個人資料蒐集、處理或利用過程，應檢視個人資料是否正確，並應主動或依當事人之請求更正或補充之。

2、 各部門於發現個人資料不正確時，應適時更正或補充個人資料，並通知曾提供利用之對象及當事人。

3、 個人資料正確性有爭議者，各部門應主動或依當事人之請求停止處理或利用，但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

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。

4、 個人資料事故

個人資料事故指個人資料被竊取、竄改、毀損、滅失及洩漏，依其對本公司之衝擊分為以下二個等級:

(1) 第一級個人資料事故:

A. 經媒體揭露與公司有關之個人資料事故。

B. 經由媒體揭露相對第三人之個人資料事故發生損及公司重大權益之事件。

C. 其他影響旅客、投資人等相對第三人權益或形象之重大個人資料事故事件。

(2) 第二級個人資料事故: 指第一級以外之個人資料事故。

(3) 第一級個人資料事故之應變程序應依緊急事件應變管理辦法為之；第二級個人資料事故之應變程序應依本辦法為之。

(二)通報程序

個人資料事故訊息接收者由電話、E-mail、傳真等方式接收到個人資料事故訊 息後,應立即通報管理部，由管理部判斷事故等級。如屬第二級事故，應立即聯繫權責單位及交通部觀光局，並由權責單位與通報人或當事人聯絡，明確了解個人資料事故狀況。

(1) 管理部應填寫「個人資料通報單」記錄個資事故之等級，及事故之狀況，以呈報總經理。

(2) 並另視事件影響與衝擊程度，必要時得召開執行小組會議或召集相關部門並啟動事故應變程序。

(三)事故應變程序

第一級個人資料事故之應變程序應依緊急事件應變管理辦法為之。

第二級個人資料事故之應變，應依下列程序辦理。

(1) 由管理部接獲前項通知並通報總經理及交通部觀光局後，召集相關部門召開執行小組會議協助個資事故調查。

(2) 個資事故調查後，如本公司有違反個人資料保護法之規定，致個人資料被竊取、洩漏、竄改或其他侵害者，本公司應採取危害初步控管，以及相關措施終止或減緩個資事件持續擴大，並應依個人資料保護法第 12 條以適當方式通知當事人,於有必要時得視情況通報有關單位。

(3) 權責單位依執行小組會議討論結果處理個人資料事故，應盡速處理並追蹤情形，針對個人資料事故案件，以簽呈方式出具檢討報告及改善計畫，經總經理核決後施行，以確保事件完整結案。結案之「個人資料通報單」交由管理部備查。

(4) 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。

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) 電子資料安全防護措施

個人資料以電子方式保存時，應依據資訊安全管理政策、防火牆及 WAF 防護政策、電腦病毒防

禦政策、電子郵件服務使用規範、電腦資訊管理辦法、資訊報廢管理辦法、資訊系統災害復原管理辦法等相關辦法進行安全防護。

(5) 重要個人資料應另加設管控密碼，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，並依據個人資料之保存年限進行保存。於傳輸時，應指派人員親自交付，並應視情形進行密件標示處理。如需透過郵遞傳輸時，應以掛號方式寄出，並應以膠帶密封保護。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。

（二）員工管理

1、 本公司依業務需求，得適度設定所屬員工不同之權限，以控管其個人資料之情形。

2、 本公司員工每 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、 員工或承攬執行接待或引導旅客觀光旅遊業務而收取報酬之導遊、領隊。與公司終止僱傭、委任、承攬等契約時，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（在任職時之相關勞務契約已有所約定時，亦屬之）。

4、 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。

5、 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）。

6、 本公司應於聘僱合約中規範員工應負保密義務，並應

確認個人資料蒐集、處理與利用之人員係依作業之需要，以設定人員存取個人資料檔案之權限及管制人員接觸個人資料之情形。各項人員管理方式如下：

(1) 電子檔案:依作業之需要設定人員電腦存取權限並注意及防範異常存取或大量截取的情況。

(2) 紙本檔案:各部門應妥善保管個資文件，如有非正常作業之需而有跨部門個資文件調閱之需求時，應填寫「部門文件調閱紀錄表」,並經個資文件保管部門主管核准後始可調閱。

(3) 個資文件:如需送倉庫儲存、調閱，各部門應填寫「文件倉儲工作單」,經個資文件保管部門主管核准後始可進行。如需銷毀，應填寫「資料/文件銷毀單」,並經個資文件保管部門主管核准後始可進行。

(4) 於人員離職時，應依人事薪資管理辦法完成職務移交手續，並刪除離職人員之各項電腦權限。

（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、 本公司之旅客個人資料檔案應定期備份。

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。

7、 本公司依據設備之不同，實施適宜之安全管制方式。行政類設備之安全管理依據資產管理辦法等相關辦法進行安全管理。資訊類設備之安全管理依據資訊安

全管理政策、防火牆及 WAF 防護政策、電腦病毒防禦政策、電子郵件服務使用規範、電腦資訊管理辦法、資訊報廢管理辦法、資訊系統災害復原管理辦法等相關辦法進行安全管理。

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。

4、 前述查察情形及結果應載入稽核報告中，由總召集人簽名確認。

（二） 內部稽核人員訂定年度稽核計畫應包含資訊系統循環及資通安全檢查，並依計畫執行稽核工作與撰寫稽核報告並呈董事長核准；若發現內控缺失及異常事項，應加以追蹤並做成追蹤改善報告，經適當之權責主管複核，並適時予以解決，並於董事會提出報告，以確保內部控制制度執行之有效性。

（三） 內部稽核人員每年應將個人資料保護之管理列入稽核計畫並進行查核，稽核報告呈總召集人複核，如有缺失則通知各受查單位改善，並做成追蹤報告經總召集人複核，以確定其已即時採取適當之改善措施

八、 使用記錄、軌跡資料及證據保存

（一）本公司應建立個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存，以證明落實本辦法之規定。

（二）前項紀錄、資料或證據之保存期限，除法令另有規定外，應至少保存五年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

九、 認知宣導及教育訓練

（一） 認知宣導

1、 本公司每年派遣員工2人參與交通部觀光局辦理進行個人資料保護法基礎教育宣導及數位學習教育訓練至少2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

2、 管理部應對本公司所屬人員施以認知宣導且每年應至少辦理一次個人資料保護與管理相關教育訓練，併同緊急應變管理程序一同演練，以提升員工個人資料保護意識。

（二） 教育訓練

1、 前項之教育訓練內容應包含個人資料保護相關法令之規定、本公司所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

2、 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

管理部應參酌業務執行狀況、社會輿情、技術發展、法令變動等因素，檢視本辦法是否合宜，必要時予以修正。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

（一） 公司業務終止之定義，指部門裁撤或法人消滅之情形。

（二） 業務終止後，針對個人資料所採取之措施為銷毀或移轉，並應留存相關紀錄。如為部門裁撤，其個人資料可透過簽呈註明移轉方法、移轉對象、移轉地點，經董事長核准後，得移轉至公司其他部門使用。如為法人消滅，其個人資料除法令規定應予以保存之文件外，其他相關個人資料文件之銷毀，應依個人資料刪除/銷毀程序辦理。如為法人被收購之情形而有移轉個人資料之必要，應以適當方式告知當事人，並留存相關紀錄。

（三） 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）：

1、 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：

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）。

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。

移轉之原因：

□業務需求。

■其他：結束營業

移轉之對象：無

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：銷毀

移轉之時間：結束營業日。

移轉之地點：本公司。

受移轉對象得保有該項個人資料之合法依據：已銷毀

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。

其他刪除、停止處理或利用之方法：依前述規定辦理。

其他刪除、停止處理或利用之時間：依前述規定辦理。

其他刪除、停止處理或利用之地點：依前述規定辦理。

十二、 實施與修訂

（一） 本辦法之制定經呈董事長核准後實施，修改時亦同。

（二） 本辦法制定日期：102 年 8 月 30 日，並自 102 年 9 月 1 日起實施。

（三） 本辦法第 2 版修訂日期：104 年 10 月 26 日，並自 104 年 11 月 01 日起實施。

拾參、表單

（一） 個人資料通報單。

（二） 部門文件調閱紀錄表。

（三） 文件倉儲工作單。

（四） 資料及文件銷毀單。

拾肆、附件

附圖。

拾伍、相關辦法

無。