

大宇資訊股份有限公司

個人資料管理程序

壹、前言：

為確保本公司所有之個人資料檔之安全，依規定制訂本程序以維護個人資料檔案之安全事項。

貳、適用範圍：

本程序規範係針對蒐集、處理、利用及國際傳輸個人資料之事項，訂定相關規範事項，以建立個人資料管理制度，確保個人資料之安全。

參、本公司應成立管理組織，並配置相當資源。

肆、界定個人資料之範圍

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、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、聯絡方式、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。

二、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。

伍、個人資料之風險評估及管理機制

一、應建立資訊系統資產等級之分類，以及相對應之管控層級作業。

二、所有資訊系統資產的新增、刪除與修改皆須保存記錄，並依其所應保存層級保存之。

陸、事故之預防、通報及應變機制

本公司應建立事故之預防、通報及應變之適當程序，使風險降至最低。

(一) 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。

(二) 查明事故之狀況並以適當方式通知當事人。

(三) 研議預防機制，避免類似事故再次發生。

柒、個人資料蒐集、處理及利用之內部管理程序。

本公司所有個人資料的蒐集、處理及利用之控管程序，應依據本公司核可標準及符合主管機關相關法規規定訂定之。

- 一、蒐集：指以任何方式取得個人資料，本公司依法均須踐行相關法定告知義務。
- 二、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，應依相關安全維護措施執行。
- 三、利用：指將蒐集之個人資料為處理以外之使用，應經過適當審核程序始可進行。
- 四、委託他人蒐集、處理、利用個人資料之全部或一部時，應對受託人為適當之監督，並明確約定相關監督事項與方式。

捌、資料安全管理及人員管理。

一、資料安全方面

- (一) 個人資料檔案建置在資料庫上者，應釐定使用範圍及使用權限「使用者代碼」、「識別密碼」，識別密碼應保密，不得與他人共用。
- (二) 個人資料檔案儲存在個人電腦硬式磁碟機上者，資料保有單位應在該個人電腦設置開機密碼、螢幕保護程式密碼及相關安全措施。
- (三) 非經允准不得使用個人資料檔案。
- (四) 個人資料檔案使用完畢應即退出，不得留置在電腦顯示畫面上。
- (五) 個人所使用之識別密碼應予保密，且須於一固定時間後自行變更密碼，以防它人竊取並長期使用。
- (六) 若顧客或個人以電話查詢其個人資料時，需先經認證後方可回覆相關資料，以維護顧客或個人之權益。
- (七) 以網際網路蒐集、處理、國際傳遞及利用個人資料時，應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。
- (八) 以網際網路進行交易處理時，應評估可能之安全風險，並研擬妥適的安全控管措施。

二、人員管理

- (一) 以電腦處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應另行設定密碼，以利管理。
- (二) 員工離職後，其離職員工曾接觸過之密碼均需取消並作適當之調整。

玖、認知宣導及教育訓練。

本公司應不定期宣導或派員參加以個人資料保護為中心之教育訓練，包括資訊安全、隱私保護、推論控制之控制措施等課程。

拾、設備安全管理。

- 一、為保護資訊處理中心免遭實體傷害，應建立門禁管控。
- 二、系統伺服器應安置於機房內，由專人專責管理，並管制相關人員進出及記錄。
- 三、主機應安裝適當於安全偵測及防制設備、各項安全設備應依廠商的使用說明定期檢查。
- 四、本公司應制定電腦報廢程序，並確實將硬碟資料銷毀，以避免內部資料外洩。

拾壹、資料安全稽核機制。

- 一、以電腦處理個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原檔案相符。
- 二、個人資料提供使用時，應核對與檔案資料是否相符，如有疑義，應調閱原檔案查核。
- 三、應建立定期稽核制度，並保存稽核資料。

拾貳、必要之使用紀錄、軌跡資料及證據之保存。

資訊部門，針對使用公司網路資源，採取必要的網路通聯 LOG 記錄儲存。如發生個資外洩事故時，提供司法調查佐證。

拾參、個人資料安全維護之整體持續改善。

本公司應透過稽核結果、預防措施與矯正行動以及管理階層審核，持續改善個人資訊管理系統之有效性。

拾肆、附則

本辦法經總經理核准後實施，修正時亦同。