

個人資料保護及管理政策

1. 目的

本公司為落實個人資料之保護及管理，並符合「個人資料保護法」（以下簡稱個資法）之要求，特訂定個人資料保護及管理政策（以下簡稱本政策），以利同仁遵循並提升個人資料保護意識。本公司個人資料保護管理之目標如下：

- 依「個人資料保護法」、「個人資料保護法施行細則」與 ISO/IEC 27701 要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
- 為保護本公司業務相關個人資料之安全，免於因外在威脅或內部人員不當管理與使用，致遭竊取、竄改、毀損、滅失、洩漏等風險。
- 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護環境。
- 定期針對個人資料相關流程進行風險評鑑，並鑑別可承受風險等級。
- 本政策適用服務範圍為「資安監控中心服務」及「電子郵件警覺性測試服務」。
- 本公司作為 PII（個人可識別資訊）控制者及處理者，依據相關法律、規範、司法或行政裁決、合約等，訂立應盡的責任與義務。
- 本政策暨隱私權聲明將適時依據法律修正、相關技術之發展及內部管理制度之調整而配合修改。

2. 個人資料之蒐集與處理

- 本公司因營運所需取得或蒐集之個人資料，包括但不限於個人之姓名、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、職業等。
- 個人資料之蒐集、處理相關活動，應遵循我國個資法等法律、法規要求，符合目的、相關且適當、不過度，並以公平、合法為基本原則，在確實必要的範圍內處理目的所需的最低限度的個人資料。
- 若有蒐集、處理 16 歲以下兒童之個人資料，應採取較其它個資更嚴謹的保護措施。
- 本公司維持正確的個人資料，在必要處保持更新，並基於法律或法規理由的要求或合法的目的保留個人資料，確保及時與適當的處置，並保存處理個人資料之紀錄。

3. 個人資料之利用及國際傳遞

- 本公司於利用個人資料時，除需依個資法之特定目的必要範圍內為之，如欲進行特定目的以外之利用，須依個資法第二十條之規定辦理；倘有必要取得當事人同意者，本公司應依法取得。
- 本公司業務承辦同仁利用個人資料時，須確保符合特定目的且為本公司營運或業務所必需。
- 提供清楚訊息給予個資當事人（包含兒童），包含利用的方式及利用的對象
- 本公司若有利用 16 歲以下兒童之個人資料時，應採取較其它個資更嚴謹的保護措施。
- 本公司取得之個人資料如有進行國際傳遞之必要者，須依不違反國家重大利益、不以迂迴方法向第三國傳遞、不規避個資法之規定而利用個人資料等原則辦理。若國際條約或協定有特別規定，或資料接受國對個人資料之保護未有完善法令致有損害當事人權益之虞者，本公司將不進行國際傳遞，以維護個人資料之安全。個人資料若需進行國際傳遞時，則須遵循當地個資法規採取適當之保護措施。
- 在提供產品與服務給歐盟海外其他國家的人民時，對於個人資料應有適當的策略。

4. 個人資料之調閱與異動

本公司尊重當事人之個人資料的權利，接獲當事人對其個人資料之權益請求時，應依個資法及本公司所訂程序於合法範圍內履行，包括當事人請求之：

- 查詢或閱覽個人資料。
- 製給個人資料複製本。
- 個人資料補充或更正。
- 停止蒐集、處理、利用個人資料。
- 刪除個人資料。

5. 個人資料之例外應用

- 本公司對持有之個人資料負有保密義務，除下列情形外，原則上不得對第三人揭露，除非該揭露係符合個資法第二十條及相關法令規定，且第三人係以正式公文查詢：
 - ✓ 司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。
 - ✓ 其他政府機關因執行公權力所需並有正當理由者。
 - ✓ 與公眾生命、安全有關之機關（構）為緊急救助所需者。

- 本公司對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：
 - ✓ 法律明文規定。
 - ✓ 為增進公共利益所必要。
 - ✓ 為免除當事人之生命、身體、自由或財產上之危險。
 - ✓ 為防止他人權益之重大危害。
 - ✓ 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經蒐集者依其揭露方式無從識別特定之當事人。
 - ✓ 經當事人同意。
 - ✓ 有利於當事人權益。

6. 個人資料之保護

- 本公司須成立個人資料保護組織，明確定義相關人員之責任與義務。
- 本公司須建立與實施個人資料管理制度（Personal Information Management System，以下簡稱 PIMS），以落實本政策；同仁及委外廠商、合作單位應遵循 PIMS 之規範與要求，且 PIMS 之運作亦須定期審查。委外廠商或合作單位若已通過國際個資管理標準（如 ISO/IEC 27701）之驗證，可出具第三方驗證機構之證書與稽核作業證明以取代定期審查。
- 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本公司須成立「資訊安全與隱私管理暨業務永續推動小組」，依相關法令辦理個人資料檔案及個人資料清冊之安全維護與更新。
- 個人資料檔案須建立清冊及管理制度，分級分類管理，並針對接觸人員建立安全管理規範。個人資料檔案清冊需清楚說明法規依據、特定目的、個人資料生命週期各階段之管理單位與方式等。
- 為確保持有個人資料之安全，須強化個人資料檔案相關資訊系統之存取安全，防止非授權存取，以維護個人資料之隱私性，且相關安全保護機制亦須定期查核。
- 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務活動需要及重要性考量其他輔助安全措施，以保障所有個人資料的安全。
- 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，須釐清其範圍及相關調查、存取權限。

- 本公司各單位若發生個人資料檔案遭人惡意破壞、洩漏或毀損、個人資料檔案相關作業疏失等安全事故，應進行緊急因應措施，並依本公司資訊安全事故處理之規範辦理。
- 本公司係以嚴密之政策、措施保護個人資料，包括但不限於本公司同仁均須接受個資法或個資保護之教育訓練。本公司之委外廠商或合作單位均須簽訂保密契約，並使其充分知悉個人資料保護之重要性及洩露個資相關法律責任。前述人等倘有違反保密義務或洩漏個資之情事，將受嚴格之內部懲處或嚴重之違約求償，並將追究其民、刑事法律責任。
- 定期執行個資管理的內部與外部稽核，並依需求實施相關的矯正改善措施。

7. 利害關係人之參與及期許

本公司個人資料保護及管理決議事項，應納入「資訊安全與隱私管理委員會」會議報告，且會議紀錄於必要時將提報主管機關或供客戶稽核查閱。客戶及主管機關等利害關係人如有個資相關回饋事項，將列入「資訊安全與隱私管理委員會」會議之討論議題。

8. 個人資料保護政策之宣導與修訂

- 本政策應透過宣導活動使本公司全體同仁了解及遵循，相關活動需留存紀錄以確保同仁認知之有效性。
- 本政策應每年定期或因時勢變遷、法令修正等事由，進行適當審查與必要修訂，並經核准後公告實施。
- 本公司個人資料保護之相關政策、程序、作業程序、計畫、報告、表單等文件，依本公司相關文件管理之規範辦理。

9. 個人資料保護聯絡窗口

安碁資安長：李國良，電子郵件：Carven.Lee@acercsi.com，電話：02-8979-6286#6900